

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено:

на заседании кафедры

протокол № 8 от « 24 » февраля 2021 г.

Зав. кафедрой Исмагилова А.С.

Согласовано:

Председатель УМК института



Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина

Основы организации службы защиты информации

Обязательная часть

программа бакалавриата

Направление подготовки

10.03.01 Информационная безопасность

Профиль подготовки

Организация и технология защиты информации

(в системе государственного и муниципального управления)

Квалификация

бакалавр

Разработчик (составитель)
к.ф.-м.н., доцент



/И.А. Шагапов

Для приема: 2021 г.

Уфа – 2021

Составитель: доцент Шагапов Илдар Ахняфович

Рабочая программа дисциплины утверждена на заседании кафедры, протокол № 8 от «24» февраля 2021 г.

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций	4
2. Цель и место дисциплины в структуре образовательной программы	4
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)	4
4. Фонд оценочных средств по дисциплине	5
4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине	5
4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине	6
5. Учебно-методическое и информационное обеспечение дисциплины	31
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	31
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы	31
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	32

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.7 Знать этапы, принципы и методы формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты.	Знает этапы, принципы и методы формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты.
		ОПК-10.8 Уметь в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.	Умеет в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.
		ОПК-10.9 Владеть принципами и методами формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты	Владеет принципами и методами формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Основы организации службы защиты информации» относится к группе дисциплин обязательной части образовательной программы.

Дисциплина изучается на 3 курсе в 5 семестре.

Целью учебной дисциплины «Основы организации службы защиты информации» является изучение структуры, логической организации и системы управления службой защиты информации как основного звена системы защиты информации

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий,

учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
ОПК-10.7 Знать этапы, принципы и методы формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты.	Знает этапы, принципы и методы формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты.	Не знает этапы, принципы и методы формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты.	Знает некоторые этапы, принципы и методы формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты, допускает ошибки	Частично знает этапы, принципы и методы формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты.	Знает этапы, принципы и методы формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты.
ОПК-10.8 Уметь в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности,	Умеет в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять	Не умеет в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.	Умеет в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты, допускает	Частично умеет в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности,	Умеет в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять

управлять процессом их реализации на объекте защиты.	процессом их реализации на объекте защиты.		кает ошибки	управлять процессом их реализации на объекте защиты.	процессом их реализации на объекте защиты.
ОПК-10.9 Владеть принципами и методами формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты	Владеет принципами и методами формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты	Не владеет принципами и методами формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты	Владеет некоторыми принципами и методами формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты, допускает ошибки	Частично владеет принципами и методами формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты	Владеет принципами и методами формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
<p>ОПК-10.8 Уметь в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.</p> <p>ОПК-10.9 Владеть принципами и методами формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты</p> <p>ОПК-10.8 Уметь в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и</p>	<p>Умеет в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.</p>	<p>Письменная контрольная работа 1,2 Практическое задание 1,2,3,4 Лабораторная работа 1,2,3,4</p>
	<p>Владеет принципами и методами формирования политики информационной безопасности, организации, поддержки и выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты</p>	<p>Письменная контрольная работа 1,2 Практическое задание 1,2,3,4 Лабораторная работа 1,2,3,4</p>
	<p>Умеет в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению</p>	<p>Письменная контрольная работа 1,2 Практическое задание 1,2,3,4 Лабораторная работа 1,2,3,4</p>

поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.	информационной безопасности, управлять процессом их реализации на объекте защиты.	
--	---	--

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (*для экзамена*: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; *для зачета*: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

(*для экзамена*:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

Рейтинг – план дисциплины

Основы организации службы защиты информации

Направление подготовки 10.03.01 ИБ

Курс 3, семестр 5

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №1	5	1	0	5
3. Практическая работа №2	5	1	0	5
Рубежный контроль				
1. Письменная контрольная работа №1	5	1	0	5
1. Лабораторная работа №1	5	1	0	5
2. Лабораторная работа №2	5	1	0	5
Всего				35
Модуль 2.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №3	5	1	0	5
3. Практическая работа №4	5	1	0	5
Рубежный контроль				
1. Письменная контрольная работа №3	5	1	0	5
1. Лабораторная работа №3	5	1	0	5
2. Лабораторная работа №4	5	1	0	5
Всего				35
Поощрительные баллы				
1. Студенческая олимпиада			0	3

2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен				30

Комплект практических и письменных контрольных работ

Для закрепления на практике умений предусмотрены несколько практических и письменных контрольных работ.

Модуль 1

Практическая работа №1

Проектирование структуры службы защиты информации

Цель - спроектировать структуру службы защиты информации

Задание.

1. Спроектировать службу информационной безопасности предприятия информационного объекта и коротко описать функциональные обязанности по 4 (на выбор) из представленных должностей.

Функциональные подразделения и должностные лица
1. Директор
2. Начальник службы защиты информации
3. Аналитик
4. Юрист
5. Сотрудники сектора обеспечения безопасности, экономической разведки, промышленной контрразведки
6. Сотрудники сектора технической защиты
7. Сотрудники сектора охраны и режима
8. Администратор безопасности системы
9. Сотрудник группы безопасности.

2. Начертить структуру службы защиты информации.
3. Оформленный отчет о проделанной работе в электронном виде. Приветствуется использование фото, схем, таблиц и т.д.
4. Защитить работу.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	2
Выполнены 100%	5
Максимальный балл	5

Практическая работа №2

Организационные основы и принципы деятельности службы защиты информа-

ции

Задачи.

Цель – для конкретного информационного объекта определить задачи, функции службы информационной безопасности

1. Перечислить:

- принципы службы информационной безопасности;
- функции деятельности службы;
- организационно-правовой статус службы безопасности;
- Разработать перечень задач для службы информационной безопасности для конкретного предприятия (см. Приложение), сформировать список защищаемой информации, угроз безопасности информации ;
- Определить функции отдела информационной безопасности для вашей организации;
- Перечислить общие принципы деятельности службы;
- Перечислить общие виды гарантий безопасности объектов защиты;

Приложение:

Транспортно экспедиционная компания
Сфера деятельности:

- Международные грузоперевозки
- Железнодорожные грузоперевозки
- Таможенное оформление

Транспортно экспедиционная компания должна удовлетворять следующим требованиям:

- Быстрая и четкая обработка поступающих заказов.
 - Поиск и предоставления автотранспорта в заданные сроки.
 - Неукоснительное соблюдение всех правил и условий транспортировки груза. Контроль за исполнением и информирование клиента о статусе перевозки груза.
 - Формирование отчетности и прочих финансовых, сопроводительных документов.
 - Строгое соблюдение законодательства.
2. Оформленный отчет о проделанной работе в электронном виде. Приветствуется использование фото, схем, таблиц и т.д.
3. Защитить работу.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	2
Выполнены 100%	5
Максимальный балл	5

Практическая работа №3

Организационные основы и принципы деятельности службы защиты информации. Пакет документов

Цель – разработать пакет нормативных документов, необходимых для работы службы защиты информации вашей организации

Задание

1. Перечислите документы, необходимые для обеспечения полноценной организационной и правовой защиты информации;

2. Приведите примеры дополнений необходимых документов, затрагивающих вопросы, связанные с защитой информации;
 3. Разработайте документы, необходимые для работы службы безопасности, вашей организации.
- Оформленный отчет о проделанной работе в электронном виде. Приветствуется использование фото, схем, таблиц и т.д.
- Защитить работу.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	2
Выполнены 100%	5
Максимальный балл	5

Модуль 2

Практическая работа №4

Организация информационно-аналитической работы

Цель – проанализировать организацию информационно-аналитической работы.

Задание.

1. Определить цели и задачи информационно-аналитической работы;
 2. Определить направления аналитической работы;
 3. Перечислить этапы выполнения информационно-аналитических исследований производственных ситуаций;
 4. Определить методы выполнения аналитических исследований
- Оформить отчет.
- Защитить работу

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	2
Выполнены 100%	5
Максимальный балл	5

Письменная контрольная работа №1

Тест «Оплата и стимулирование труда»

Цель - провести тест «Оплата и стимулирование труда» для проверки своих знаний и уточнения собственной концепции

Тест

Вам предлагаются 13 вопросов, каждый из которых имеет три варианта ответов. Выберите наиболее правильный с Вашей точки зрения и выпишите его числовой индекс (1.2, 6.3 и т.д.). По таблице оценок присвойте каждому ответу установленное число очков и подведите итог. Поскольку некоторые вопросы связаны с определенными концепциями и могут быть неоднозначны, Вы можете прибавить себе 2 очка, если готовы обосновать, что Ваш ответ основывается на общем подходе к проблеме.

Тест «Оплата и стимулирование труда»

1. Оплата труда:

- 1.1 Всегда главный стимул работы
- 1.2 Второстепенный стимул для творческих работников
- 1.3 Один из стимулов, занимающий приоритетное место при отсутствии заработка, обеспечивающего основные потребности
2. Заработная плата:
 - 2.1 Отражает личные факторы, связанные с квалификацией и условиями труда и т.д.
 - 2.2 Должна зависеть только от производительности труда сотрудника
 - 2.3 Зависит только от должности
3. Объем заработной платы:
 - 3.1 Зависит от производительности труда
 - 3.2 Зависит от производительности труда и стратегии организации
 - 3.3 Зависит от индивидуального подхода руководителя
4. Размер вознаграждения:
 - 4.1 Зависит от должности, учреждения, где он работает, принятой системы вознаграждения
 - 4.2 Зависит только от наличия дополнительных источников финансирования
 - 4.3 Зависит только от стажа и квалификации
5. Тарифно-аттестационная форма оплаты труда:
 - 5.1 Не может быть поощрительной
 - 5.2 Относится к поощрительным системам
 - 5.3 Поощряет ограниченно, нуждается в дополнении
6. Размер заработной платы должен:
 - 6.1 Зависеть только от индивидуального вклада
 - 6.2 Зависит от результатов деятельности организации и индивидуального вклада
 - 6.3 Зависит от результатов общей деятельности всего учреждения.
7. Система оплаты труда менеджера:
 - 7.1 Самостоятельная система
 - 7.2 Не отличается по своим принципам от оплаты других сотрудников
 - 7.3 Часть общей системы, имеющая свои существенные особенности
8. Единая тарифная сетка по оплате труда работников бюджетной сферы:
 - 8.1 Утверждается Правительством РФ
 - 8.2 Утверждается только первый разряд
 - 8.3 Является рекомендательным документом
9. Для изменения окладов работникам бюджетной сферы:
 - 9.1 Директивно изменяют коэффициенты по разрядам
 - 9.2 Директивно изменяют минимальный разряд
 - 9.3 Директивно изменяют высшие разряды
10. Стимулирование труда:
 - 10.1 Основывается на комплексе экономических факторах
 - 10.2 Основывается на комплексе экономических, организационных и психологических факторов
 - 10.3 В разных организациях к процессу подходят абсолютно по-разному
11. Утверждение, что низкая оплата унижает человека:

11.1 Всегда справедливо

11.2 В зависимости от субъективной оценки человека

11.3 Человек, занятый творческим, содержательным трудом, должен получать соответствующее вознаграждение, но его низкий уровень не может унижить личность

12. Дополнительное вознаграждение:

12.1 Должно быть одинаковым в масштабе организации

12.2 Должно зависеть от должностных обязанностей

12.3 Должно быть основано на общих принципах и дифференцироваться по группам работников и индивидуальной мотивации

13. Система стимулирования труда:

13.1 Должна быть раз и навсегда установлена в организации

13.2 Должна периодически пересматриваться

13.3 Стимулирование труда не система, а реакция на особые достижения

Таблица оценок к тесту «Оплата и стимулирование труда»

1	2	1	1	1	3
.1	очка	.2	очка	.3	очка
2	3	2	2	2	1
.1	очка	.2	очка	.3	очка
3	2	3	3	3	10
.1	очка	.2	очка	.3	чка
4	3	4	2	4	2
.1	очка	.2	очка	.3	очка
5	1	5	2	5	3
.1	очка	.2	очка	.3	очка
6	1	6	2	6	3
.1	очка	.2	очка	.3	очка
7	2	7	1	7	3
.1	очка	.2	очка	.3	очка
8	3	8	2	8	1
.1	очка	.2	очка	.3	очка
9	2	9	3	9	1
.1	очка	.2	очка	.3	очка
1	2	1	3	1	1
0.1	очка	0.2	очка	0.3	очка
1	1	1	2	1	3
1.1	очка	1.2	очка	1.3	очка
1	1	1	2	1	3
2.1	очка	2.2	очка	2.3	очка
1	2	1	3	1	1
3.1	очка	3.2	очка	3.3	очка

39-36 очков – Вы продемонстрировали отличные знания и у Вас есть единая концепция по проблеме оплаты и стимулирования труда. Скорее всего, Вы готовы к соответствующей работе в структуре управления персоналом.

35-32 очков – Вы показали хорошие знания, но они не выстроились в целостную систему. Возможно, что Ваш подход к проблеме носит ситуационный характер и в определенных условиях может быть оправдан.

31-28 очков – Ваши знания можно оценить удовлетворительной оценкой. Возможно,

Вы слишком консервативны или не придаете должного значения проблеме. Рекомендуем пройти тест еще раз.

Менее 27 очков – Вы показали неудовлетворительное знание темы.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	3
Выполнены 100%	5
Максимальный балл	5

Письменная контрольная работа №2

Кадровое обеспечение службы информационной безопасности

Цель – Рассчитать фактическую доля сотрудников службы информационной безопасности в общей численности работников завода.

Задание.

На основании нижеприведенного примера рассчитать плановую численность каждой подсистемы службы информационной безопасности.

Построить оперограмму заданной управленческой процедуры.

Определить общую численность службы информационной безопасности машиностроительного завода; провести сравнение с данными отечественных и зарубежных предприятий.

При расчетах необходимо учесть: полезный фонд рабочего времени – 1940 ч/год; коэффициент дополнительных затрат времени – 1,15.

Плановая трудоемкость:

1. Наем, подбор и учет персонала – 11510 ч/год;
2. Развитие персонала – 8230 ч/г;
3. Планирование и маркетинг персонала – 13600 ч/г;
4. Разработка средств стимулирования труда – 10110 ч/г;
5. Трудовые отношения – 5108 ч/г;
6. Условия труда – 6120 ч/г;
7. Социальной инфраструктуры – 13380 ч/г;
8. Юридических услуг -2070 ч/г.

Фактическая численность персонала в подразделениях:

1. Наем, подбор и учет персонала – 8 чел;
2. Развитие персонала – 3 чел;
3. Планирование и маркетинг персонала – 9 чел;
4. Разработка средств стимулирования труда – 7 чел;
5. Трудовые отношения – 3 чел;
6. Условия труда – 5 чел;
7. Социальной инфраструктуры – 8 чел;
8. Юридических услуг – 1 чел.

Таблица 2.1. Исходные данные
Численность

1	2	3	4	5	6	7	8	9	10
4	4	3	3	4	1	2	3	4	3

300	000	300	000	500	500	000	500	200	050
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

Таблица 2.2. Исходные данные

Вариант	Управленческие процедуры
1	Подбор персонала
2	Адаптация персонала
3	Планирование потребности в персонале
4	Планирование обучения персонала
5	Увольнение персонала

Расчет плановой численности проведем по формуле:

1. Наем, подбор и учет персонала – $11510 \cdot 1,15 / 1940 = 7$ чел;
2. Развитие персонала – $8230 \cdot 1,15 / 1940 = 5$ чел;
3. Планирование и маркетинг персонала – $13600 \cdot 1,15 / 1940 = 8$ чел;
4. Разработка средств стимулирования труда – $10110 \cdot 1,15 / 1940 = 6$ чел;
5. Трудовые отношения – $5108 \cdot 1,15 / 1940 = 3$ чел; 6. Условия труда – $6120 \cdot 1,15 / 1940 = 4$ чел;
7. Социальной инфраструктуры – $13380 \cdot 1,15 / 1940 = 8$ чел;
8. Юридических услуг – $2070 \cdot 1,15 / 1940 = 1$ чел. Наблюдается

перекос в плановой численности персонала:

1. Наем, подбор и учет персонала – 1 человек лишний;
2. Развитие персонала – 2 человека недостает;
3. Планирование и маркетинг персонала – 1 человек лишний;
4. Разработка средств стимулирования труда – 1 человек лишний;
5. Условия труда – 1 человек лишний;

Построение оперограммы приведено в таблице 2.3.

Таблица 2.3. Оперограмма адаптации персонала.

№ п /п	Операции	Исполнитель			Трудо- емкость На единицу объема ра- боты, дн.	О бъем рабо- ты в г оду	Общая трудоем- кость в году
		Со- трудник	Руково- дитель	Отдел кадров			
1	Помощь в оформлении документов	По- дача заявле- ния и др.			0,1	5	0,5
2	Ознаком- ление				0,2	5	1
3	Закрепление наставника				0,1	5	0,5

4	Беседа с персоналом : Проведение беседы с сотрудниками, получение их впечатлений о работе и условиях труда			Предоставление новому сотруднику наставника	0,15	2	1	1,8
5	Выявление недостатков и их устранение, внесение изменений в организацию труда с целью повышения привлекательности труда			Представление сотруднику его рабочего места. Оформление анкет и документов	0,5	5	1	7,5
Всего								11,3

Рассчитаем общую численность службы информационной безопасности.

Таблица 2.4. Общее число сотрудников службы управления.

Подразделение	Численность
1. Наем, подбор и учет персонала	8
2. Развитие персонала	3
3. Планирование и маркетинг персонала	9
4. Разработка средств стимулирования труда	7
5. Трудовые отношения	3
6. Условия труда	5
7. Социальной инфраструктуры	8
8. Юридических услуг	1
Итого:	44

Фактическая доля сотрудников службы информационной безопасности в общей численности работников завода составит:

$$4200/44=95 \text{ человек}$$

Т.е. на 1 работника службы ИБ приходится 95 работников завода, по усредненным показателям (1,0-1,2% от числа персонала предприятия) число работников службы безопасности должно составлять 46 человек, на 1 сотрудника службы ИБ должно приходиться 91 работник предприятия.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	3
Выполнены 100%	5
Максимальный балл	5

Комплект лабораторных работ

Для закрепления на практике умений предусмотрены несколько лабораторных работ.

Лабораторная работа №1

Проектирование структуры службы защиты информации

Цель - спроектировать структуру службы защиты информации

Задание.

1. Спроектировать службу информационной безопасности предприятия информационного объекта и коротко описать функциональные обязанности по 4 (на выбор) из представленных должностей.

Функциональные подразделения и должностные лица
1. Директор
2. Начальник службы защиты информации
3. Аналитик
4. Юрист
5. Сотрудники сектора обеспечения безопасности, экономической разведки, промышленной контрразведки
6. Сотрудники сектора технической защиты
7. Сотрудники сектора охраны и режима
8. Администратор безопасности системы
9. Сотрудник группы безопасности.

2. Начертить структуру службы защиты информации.
3. Оформленный отчет о проделанной работе в электронном виде. Приветствуется использование фото, схем, таблиц и т.д.
4. Защитить работу.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	3
Выполнены 100%	5
Максимальный балл	5

Лабораторная работа №2

Организационные основы и принципы деятельности службы защиты информации. Пакет документов

Цель – разработать пакет нормативных документов, необходимых для работы службы защиты информации вашей организации

Задание

1. Перечислите документы, необходимые для обеспечения полноценной организационной и правовой защиты информации;
2. Приведите примеры дополнений необходимых документов, затрагивающих вопросы, связанные с защитой информации;

3. Разработайте документы, необходимые для работы службы безопасности, вашей организации.
- Оформленный отчет о проделанной работе в электронном виде. Приветствуется использование фото, схем, таблиц и т.д.
 - Защитить работу.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	3
Выполнены 100%	5
Максимальный балл	5

Лабораторная работа №3

Организация информационно-аналитической работы

Цель – проанализировать организацию информационно-аналитической работы.

Задание.

1. Определить цели и задачи информационно-аналитической работы;
 2. Определить направления аналитической работы;
 3. Перечислить этапы выполнения информационно-аналитических исследований производственных ситуаций;
 4. Определить методы выполнения аналитических исследований
- Оформить отчет.
 - Защитить работу

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	3
Выполнены 100%	5
Максимальный балл	5

Лабораторная работа №4

Разработка технического задания (ТЗ) на создание системы защиты информации предприятия

1. Изучить деятельность выбранного (гипотетически придуманного) предприятия.
2. Собрать необходимую информацию по предприятию.
3. Составить техническое задание на создание системы защиты информации предприятия.

Методические указания

- а. Изучить ГОСТ по написанию ТЗ и образцы готовых вариантов.
- б. Помнить, для чего и для кого разрабатывается ТЗ.

Теоретическая часть

Разработка программы: пример технического задания

1. Введение
 - 1.1. Наименование программы
Наименование программы: "Тестовая программа"
 - 1.2. Назначение и область применения

Программа предназначена для ...

2. Требования к программе

2.1. Требования к функциональным характеристикам

Программа должна обеспечивать возможность выполнения перечисленных ниже функций:

2.2. Требования к надежности

2.2.1 Требования к обеспечению надежного функционирования программы

Надежное (устойчивое) функционирование программы должно быть обеспечено выполнением Заказчиком совокупности организационно-технических мероприятий, перечень которых приведен ниже:

а) организацией бесперебойного питания технических средств;

б) использованием лицензионного программного обеспечения;

в) регулярным выполнением рекомендаций Министерства труда и социального развития РФ, изложенных в Постановлении от 23 июля 1998 г.

Об утверждении межотраслевых типовых норм времени на работы по сервисному обслуживанию ПЭВМ и оргтехники и сопровождению программных средств»;

г) регулярным выполнением требований ГОСТ 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов

2.2.2. Время восстановления после отказа

Время восстановления после отказа, вызванного сбоем электропитания технических средств (иными внешними факторами), не фатальным сбоем (не крахом) операционной системы,

не должно превышать 30-ти минут при условии соблюдения условий эксплуатации технических и программных средств.

Время восстановления после отказа, вызванного неисправностью технических средств, фатальным сбоем (крахом) операционной системы, не должно превышать времени, требуемого на устранение неисправностей технических средств и переустановки программных средств.

2.2.3. Отказы из-за некорректных действий оператора

Отказы программы возможны вследствие некорректных действий оператора (пользователя) при взаимодействии с операционной системой.

Во избежание возникновения отказов программы по указанной выше причине следует обеспечить работу конечного пользователя без предоставления ему административных привилегий

3. Условия эксплуатации

3.1. Климатические условия эксплуатации

Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики, должны удовлетворять требованиям,

предъявляемым к техническим средствам в части условий их эксплуатации

3.2. Требования к квалификации и численности персонала

Минимальное количество персонала, требуемого для работы программы, должно составлять не менее 2 штатных единиц — системный администратор и конечный пользователь программы — оператор.

Системный администратор должен иметь высшее профильное образование и сертификаты компании-производителя операционной системы. В перечень задач, выполняемых системным администратором, должны входить:

а) задача поддержания работоспособности технических средств;

б) задачи установки (инсталляции) и поддержания работоспособности системных программных средств — операционной системы;

в) задача установки (инсталляции) программы.

г) задача создания резервных копий базы данных.

3.3. Требования к составу и параметрам технических средств

3.3.1. В состав технических средств должен входить IBM-совместимый персональный компьютер (ПЭВМ), выполняющий роль сервера, включающий в себя:

3.3.1.1. процессор Pentium-2.0Hz, не менее;

3.3.1.2. оперативную память объемом, 1Гигабайт, не менее;

3.3.1.3. оперативную память объемом, 1Гигабайт, не менее;

3.3.1.4. операционную систему Windows 2000 Server или Windows 2003;

3.3.1.5. операционную систему Windows 2000 Server или Windows 2003;

3.3.1.6. Microsoft SQL Server 2000

3.4. Требования к информационной и программной совместимости

3.4.1. Требования к информационным структурам и методам решения

База данных работает под управлением Microsoft SQL Server. Используется много поточный доступ к базе данных. Необходимо обеспечить одновременную работу с программой с той же базой данной модулей экспорта внешних данных.

3.4.2. Требования к исходным кодам и языкам программирования

Дополнительные требования не предъявляются

3.4.3. Требования к программным средствам, используемым программой

Системные программные средства, используемые программой, должны быть представлены лицензионной локализованной версией операционной системы Windows 2000 Server или Windows 2003 и Microsoft SQL Server 2000

3.4.4. Требования к защите информации и программ

Требования к защите информации и программ не предъявляются

3.5. Специальные требования

Специальные требования к данной программе не предъявляются

4. Требования к программной документации

4.1. Предварительный состав программной документации

Состав программной документации должен включать в себя:

4.1.1. техническое задание;

4.1.2. программу и методики испытаний;

4.1.3. руководство оператора;

5. Техничко-экономические показатели

5.1. Экономические преимущества разработки

Ориентировочная экономическая эффективность не рассчитываются. Аналогия не проводится ввиду уникальности предъявляемых требований к разработке.

6. Стадии и этапы разработки

6.1. Стадии разработки

Разработка должна быть проведена в три стадии:

1. разработка технического задания;

2. рабочее проектирование;

3. внедрение.

6.2. Этапы разработки

На стадии разработки технического задания должен быть выполнен этап разработки, согласования и утверждения настоящего технического задания.

На стадии рабочего проектирования должны быть выполнены перечисленные ниже этапы работ:

1. разработка программы;

2. разработка программной документации;

3. испытания программы.

На стадии внедрения должен быть выполнен этап разработки подготовка и передача программы

6.3. Содержание работ по этапам

На этапе разработки технического задания должны быть выполнены перечисленные ниже работы:

1. постановка задачи;
2. определение и уточнение требований к техническим средствам;
3. определение требований к программе;
4. определение стадий, этапов и сроков разработки программы и документации на неё;
5. согласование и утверждение технического задания.

На этапе разработки программы должна быть выполнена работа по программированию (кодированию) и отладке программы.

На этапе разработки программной документации должна быть выполнена разработка программных документов в соответствии с требованиями к составу документации.

На этапе испытаний программы должны быть выполнены перечисленные ниже виды работ:

1. разработка, согласование и утверждение методик испытаний;
2. проведение приемо-сдаточных испытаний;
3. корректировка программы и программной документации по результатам испытаний.

На этапе подготовки и передачи программы должна быть выполнена работа по подготовке и передаче программы и программной документации в эксплуатацию на объектах Заказчика.

7. Порядок контроля и приемки

7.1. Виды испытаний

Приемо-сдаточные испытания должны проводиться на объекте Заказчика в оговоренные сроки.

Приемо-сдаточные испытания программы должны проводиться согласно разработанной Исполнителем и согласованной Заказчиком Программы и методик испытаний.

Ход проведения приемо-сдаточных испытаний Заказчик и Исполнитель документируют в Протоколе проведения испытаний

7.2. Общие требования к приемке работы

На основании Протокола проведения испытаний Исполнитель совместно с Заказчиком подписывает Акт приемки-сдачи программы в эксплуатацию.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1	3
Выполнены пункты 1-3	5
Максимальный балл	5

Экзаменационные билеты¹

Структура экзаменационного билета: экзаменационный билет содержит 2 теоретических вопроса.

Перечень вопросов для экзамена:

1. Концепция построения системы безопасности предприятия
2. Определение и основные понятия системы безопасности
3. Защита информации в системе безопасности предприятия
4. Концептуальные модели компонентов системы безопасности предприятия

¹Если итоговой формой контроля является зачет, то приводится перечень вопросов и критерии оценки для зачета (с учетом наличия/отсутствия модульно–рейтинговой системы оценок).

5. Принципы построения системы безопасности предприятия
6. Правовые основы деятельности службы безопасности предприятия
7. Организационно-функциональные документы системы безопасности предприятия
8. Виды нормативных документов
9. Лицензирование видов деятельности службы безопасности предприятия
10. Рекомендации по разработке уставных документов службы безопасности предприятия
11. Организационное проектирование деятельности службы безопасности предприятия
12. Основы организационного проектирования систем управления
13. Методика проектирования функционального содержания управленческой деятельности
14. Методика проектирования организационной структуры системы управления
15. Методика оформления основных документов организационного проекта системы управления
16. Структура и функции службы безопасности предприятия
17. Состав службы безопасности предприятия
18. Основные функции службы безопасности предприятия
19. Построение структурной схемы управления службой безопасности предприятия
20. Подразделения службы безопасности предприятия
21. Подразделения режима
22. Подразделение охраны
23. Специальный отдел
24. Подразделение информационно-аналитической деятельности
25. Подразделение инженерно-технической защиты
26. Служба разведки
27. Служба контрразведки
28. Организация службы защиты информации
29. Создание СЗИ
30. Структура СЗИ
31. Организационно-технические мероприятия СЗИ
32. Технические мероприятия СЗИ
33. Руководитель службы защиты информации
34. Разработка должностных инструкций для специалистов по защите информации
35. Управление службой безопасности предприятия
36. Методы управления СБП
37. Функции процессов управления СПб
38. Принципы управления СБП
39. Обеспечение деятельности службы безопасности
40. Управление безопасностью предприятия в кризисных ситуациях
41. Подбор и расстановка сотрудников службы защиты информации
42. Обучение сотрудников службы защиты информации
43. Роль персонала в системе защиты информации
44. Набор и отбор персонала в СБП
45. Требования к специалистам по защите информации
46. Организация обучения специалистов по защите информации
47. Требования к начальнику службы безопасности предприятия

Образец экзаменационного билета:

...

МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Основные функции службы безопасности предприятия
2. Роль персонала в системе защиты информации

Зав. кафедрой УИБ

А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценки (в баллах):

- **25-30 баллов** выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- **17-24 баллов** выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;

- **10-16 баллов** выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент не решил задачу или при решении допущены грубые ошибки;

- **0-10 баллов** выставляется студенту, если он отказался от ответа или не смог ответить на вопросы билета, ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

План лекционных занятий

(18 часов)

Лекция №1

Концепция построения системы безопасности предприятия (2 часа)

- 1.1 Определение и основные понятия системы безопасности
- 1.2 Защита информации в системе безопасности предприятия
- 1.3 Концептуальные модели компонентов системы безопасности предприятия
- 1.4 Принципы построения системы безопасности предприятия

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков,

М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Лекция №2

Правовые основы деятельности службы безопасности предприятия (2 часа)

- 2.1. Организационно-функциональные документы системы безопасности предприятия
- 2.2. Виды нормативных документов
- 2.3. Лицензирование видов деятельности службы безопасности предприятия
- 2.4. Рекомендации по разработке уставных документов службы безопасности предприятия

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Лекция №3

Организационное проектирование деятельности службы безопасности предприятия (2 часа)

- 3.1. Основы организационного проектирования систем управления
- 3.2. Методика проектирования функционального содержания управленческой деятельности
- 3.3. Методика проектирования организационной структуры системы управления
- 3.4. Методика оформления основных документов организационного проекта системы управления

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Лекция №4

Структура и функции службы безопасности предприятия (2 часа)

- 4.1. Состав службы безопасности предприятия
- 4.2. Основные функции службы безопасности предприятия
- 4.3. Построение структурной схемы управления службой безопасности предприятия

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Лекция №5

Подразделения службы безопасности предприятия (2 часа)

- 5.1. Подразделения режима и охраны
- 5.2. Специальный отдел
- 5.3. Подразделение информационно-аналитической деятельности
- 5.4. Подразделение инженерно-технической защиты
- 5.5. Подразделение разведки

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Лекция №6

Организация службы защиты информации(2 часа)

- 6.1. Создание СЗИ
- 6.2. Структура СЗИ
- 6.3. Организационно-технические мероприятия СЗИ
- 6.4. Руководитель службы защиты информации
- 6.5. Разработка должностных инструкций для специалистов по защите информации

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Лекция №7

Управление службой безопасности предприятия (СБП) (2 часа)

- 7.1. Методы управления СБП
- 7.2. Функции процессов управления СБП
- 7.3. Принципы управления СБП
- 7.4. Обеспечение деятельности службы безопасности
- 7.5. Управление безопасностью предприятия в кризисных ситуациях

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Лекция №8

Подбор, расстановка и обучение сотрудников службы защиты информации (2 часа)

- 8.1. Роль персонала в системе защиты информации
- 8.2. Набор и отбор персонала в СБП
- 8.3. Требования к специалистам по защите информации

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Лекция №9

Подбор, расстановка и обучение сотрудников службы защиты информации (2 часа)

- 9.1. Организация обучения специалистов по защите информации
- 9.2. Требования к начальнику службы безопасности предприятия
- 9.3. Новые подходы к кадровому обеспечению службы информационной безопасности предприятия

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Планы семинарских занятий

(36 часов)

Семинар №1-2.

Концепция построения системы безопасности предприятия (4 часа)

Вопросы:

1. Определение и основные понятия системы безопасности
2. Защита информации в системе безопасности предприятия
3. Концептуальные модели компонентов системы безопасности предприятия

Принципы построения системы безопасности предприятия

Задание. Изучить материал, подготовить устный ответ на все вопросы.

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Исмагилова А.С., Салов И.В., Шагапов И.А., Корнилова А.А. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.В. Салов, И.А. Шагапов, А.А. Корнилова. – Уфа: РИЦ БашГУ, 2019. – 128 с. URL: https://elib.bashedu.ru/dl/read/Ismagilov_i_dr_Inform_bezopasnost_v_cifr_obshchestve_mon_2019.pdf

Семинар №3-4

Правовые основы деятельности службы безопасности предприятия (4 часа)

1. Организационно-функциональные документы системы безопасности предприятия. Виды нормативных документов

2. Лицензирование видов деятельности службы безопасности предприятия
3. Рекомендации по разработке уставных документов службы безопасности предприятия

Задание. Изучить материал, подготовить устный ответ на все вопросы.

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Исмагилова А.С., Салов И.В., Шагапов И.А., Корнилова А.А. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.В. Салов, И.А. Шагапов, А.А. Корнилова. – Уфа: РИЦ БашГУ, 2019. – 128 с. URL: https://elib.bashedu.ru/dl/read/Ismagilov_i_dr_Inform_bezopasnost_v_cifr_obshchestve_mon_2019.pdf

Семинар №5-6

Организационное проектирование деятельности службы безопасности предприятия (4 часа)

1. Основы организационного проектирования систем управления
2. Методика проектирования функционального содержания управленческой деятельности
3. Методика проектирования организационной структуры системы управления
4. Методика оформления основных документов организационного проекта системы управления

Задание. Изучить материал, подготовить устный ответ на все вопросы.

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Исмагилова А.С., Салов И.В., Шагапов И.А., Корнилова А.А. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.В. Салов, И.А. Шагапов, А.А. Корнилова. –

Уфа: РИЦ БашГУ, 2019. – 128 с. URL: https://elib.bashedu.ru/dl/read/Ismagilov_i_dr_Inform_bezopasnost_v_cifr_obshchestve_mon_2019.pdf

Семинар №7-8

Структура и функции службы безопасности предприятия (4 часа)

1. Состав службы безопасности предприятия
2. Основные функции службы безопасности предприятия
3. Построение структурной схемы управления службой безопасности предприятия

Задание. Изучить материал, подготовить устный ответ на все вопросы.

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Исмагилова А.С., Салов И.В., Шагапов И.А., Корнилова А.А. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.В. Салов, И.А. Шагапов, А.А. Корнилова. – Уфа: РИЦ БашГУ, 2019. – 128 с. URL: https://elib.bashedu.ru/dl/read/Ismagilov_i_dr_Inform_bezopasnost_v_cifr_obshchestve_mon_2019.pdf

Семинар №9-10

Подразделения службы безопасности предприятия (4 часа)

1. Подразделения режима и охраны
2. Специальный отдел
3. Подразделение информационно-аналитической деятельности
4. Подразделение инженерно-технической защиты
5. Подразделение разведки

Задание. Изучить материал, подготовить устный ответ на все вопросы.

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. —

Режим доступа: <https://e.lanbook.com/book/39990>.

Исмагилова А.С., Салов И.В., Шагапов И.А., Корнилова А.А. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.В. Салов, И.А. Шагапов, А.А. Корнилова. – Уфа: РИЦ БашГУ, 2019. – 128 с. URL: https://elib.bashedu.ru/dl/read/Ismagilov_i_dr_Inform_bezopasnost_v_cifr_obshchestve_mon_2019.pdf

Семинар №11-12

Организация службы защиты информации (4 часа)

1. Создание СЗИ. Структура СЗИ
2. Организационно-технические мероприятия СЗИ
3. Руководитель службы защиты информации
4. Разработка должностных инструкций для специалистов по защите информации

Задание. Изучить материал, подготовить устный ответ на все вопросы.

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Исмагилова А.С., Салов И.В., Шагапов И.А., Корнилова А.А. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.В. Салов, И.А. Шагапов, А.А. Корнилова. – Уфа: РИЦ БашГУ, 2019. – 128 с. URL: https://elib.bashedu.ru/dl/read/Ismagilov_i_dr_Inform_bezopasnost_v_cifr_obshchestve_mon_2019.pdf

Семинар №13-14

Управление службой безопасности предприятия (СБП) (4 часа)

1. Методы управления СБП. Функции процессов управления СБП
2. Принципы управления СБП
3. Обеспечение деятельности службы безопасности
4. Управление безопасностью предприятия в кризисных ситуациях

Задание. Изучить материал, подготовить устный ответ на все вопросы.

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Исмагилова А.С., Салов И.В., Шагапов И.А., Корнилова А.А. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.В. Салов, И.А. Шагапов, А.А. Корнилова. — Уфа: РИЦ БашГУ, 2019. — 128 с. URL: https://elib.bashedu.ru/dl/read/Ismagilov_i_dr_Inform_bezopasnost_v_cifr_obshchestve_mon_2019.pdf

Семинар №15-16

Подбор, расстановка и обучение сотрудников службы защиты информации (4 часа)

1. Роль персонала в системе защиты информации
2. Набор и отбор персонала в СБП
3. Требования к специалистам по защите информации

Задание. Изучить материал, подготовить устный ответ на все вопросы.

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. — 3-е изд., стереотип. — М. : ФЛИНТА, 2016. — 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. — 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Исмагилова А.С., Салов И.В., Шагапов И.А., Корнилова А.А. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.В. Салов, И.А. Шагапов, А.А. Корнилова. — Уфа: РИЦ БашГУ, 2019. — 128 с. URL: https://elib.bashedu.ru/dl/read/Ismagilov_i_dr_Inform_bezopasnost_v_cifr_obshchestve_mon_2019.pdf

Семинар №17-18

Обучение сотрудников службы защиты информации (4 часа)

1. Организация обучения специалистов по защите информации
2. Требования к начальнику службы безопасности предприятия
3. Новые подходы к кадровому обеспечению службы информационной безопасности предприятия

Задание. Изучить материал, подготовить устный ответ на все вопросы.

Основная литература.

Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. — 3-е изд., стереотип. — М. : ФЛИНТА, 2016. — 186 с.

Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. — 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный

ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>

Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.

Исмагилова А.С., Салов И.В., Шагапов И.А., Корнилова А.А. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.В. Салов, И.А. Шагапов, А.А. Корнилова. — Уфа: РИЦ БашГУ, 2019. — 128 с. URL: https://elib.bashedu.ru/dl/read/Ismagilov_i_dr_Inform_bezopasnost_v_cifr_obshchestve_mon_2019.pdf

Критерии оценки (в баллах) (должны строго соответствовать рейтинг плану по макс. и мин. колич. баллов и только для тех, кто учится с использованием модульно-рейтинговой системы обучения и оценки успеваемости студентов):

- 0,55 баллов выставляется студенту, если выполнил задание на 100%
- 0,36 баллов выставляется студенту, если выполнил задание на 75%
- 0,2 баллов выставляется студенту, если выполнил задание на 50%
- 0 баллов выставляется студенту, если не выполнил задание

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература.

1. Аверченков В.И. Служба защиты информации : организация и управление : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 186 с.
2. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М. : Флинта, 2011. – 186 с. - [Электронный ресурс]. Режим доступа: URL: <http://biblioclub.ru/index.php?page=book&id=93356>
3. Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Дополнительная литература.

4. Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=93343>
5. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: <https://e.lanbook.com/book/39990>.
6. Исмагилова А.С., Салов И.В., Шагапов И.А., Корнилова А.А. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.В. Салов, И.А. Шагапов, А.А. Корнилова. — Уфа: РИЦ БашГУ, 2019. — 128 с. URL: https://elib.bashedu.ru/dl/read/Ismagilov_i_dr_Inform_bezopasnost_v_cifr_obshchestve_mon_2019.pdf

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Справочная правовая система «КонсультантПлюс» – <http://www.consultant-plus.ru>.
2. Электронная библиотечная система «Университетская библиотека онлайн» – <https://biblioclub.ru>.
3. Электронная библиотечная система издательства «Лань» – <https://e.lanbook.com/>

4. Электронный каталог Библиотеки БашГУ – <http://www.bashlib.ru/catalogi/>
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. <http://window.edu.ru/> – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. <http://univertv.ru/video/matematika/> – Открытый образовательный видеопортал Uni-verTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www.edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
<p>1. учебная аудитория для проведения занятий лекционного типа: аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).</p> <p>2. учебная аудитория для проведения лабораторных работ: Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус).</p> <p>3. учебная аудитория для проведения занятий</p>	<p>Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация</p>	<p style="text-align: center;">Аудитория № 403</p> <p>Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.</p> <p style="text-align: center;">Аудитория № 405</p> <p>Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTEL-Corei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMIC-MPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт.</p> <p style="text-align: center;">Аудитория № 413</p> <p>Учебная мебель, доска, двухполос-</p>	<p>1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.</p> <p>2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</p> <p>3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. Лицензии бессрочные.</p>

<p><i>семинарского типа:</i> аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус).</p> <p>4. учебная аудитория для проведения групповых и индивидуальных консультаций: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p> <p>5. учебная аудитория для текущего контроля и промежуточной аттестации: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный кор-</p>		<p>ный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p>Аудитория № 415 Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p>Аудитория № 416 Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p>Аудитория № 418 Учебная мебель, доска, Экран настенный Lumien Master Piktura 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.</p> <p>Аудитория № 419 Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p>Аудитория № 515 Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профессиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI SMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром.</p> <p>Аудитория № 516 Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p>Аудитория № 509 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 608 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 609 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 610 Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.</p>	
---	--	---	--

<p>пус).</p> <p>6. помещения для самостоятельной работы: читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).</p> <p>7.помещение для хранения и профилактического обслуживания учебного оборудования: аудитория № 523 (гуманитарный корпус).</p>		<p>Аудитория № 613 Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p>Компьютерный класс аудитория № 420 Учебная мебель, моноблоки стационарные 15 шт.</p> <p>Компьютерный класс аудитория № 404 Учебная мебель, компьютеры -15 штук.</p> <p>Аудитория 402 читальный зал библиотеки Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные.</p> <p>Лаборатория полигон технической защиты информации № 508 Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный ком-плект инструментов для проведения работ по специальным проверкам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон".</p> <p>Аудитория № 523 Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.</p>	
--	--	--	--

МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Содержание рабочей программы
дисциплины

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	55
лекций	18
практических/ семинарских	36
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	25,8
Учебных часов на подготовку к экзамену	27

Форма контроля:
экзамен 5 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СРС		
1	2	3	4	5	6	7	8
1	Концепция построения системы безопасности предприятия 1.1 Определение и основные понятия системы безопасности 1.2 Защита информации в системе безопасности предприятия 1.3 Концептуальные модели компонентов системы безопасности предприятия 1.4 Принципы построения системы безопасности предприятия	2	4		2	Изучить вопросы определения несанкционированного доступа к защищаемой информации	Письменная контрольная работа Практическое задание Лабораторная работа
2	Правовые основы деятельности службы безопасности предприятия 2.1. Организационно-функциональные документы системы безопасности предприятия 2.2. Виды нормативных документов 2.3. Лицензирование видов деятельности службы безопасности предприятия 2.4. Рекомендации по разработке уставных документов службы безопасности предприятия	2	4		2	Изучить возможности несанкционированного доступа к защищаемой информации	Письменная контрольная работа Практическое задание Лабораторная работа
3	Организационное проектирование деятельности службы безопасности предприятия 3.1. Основы организационного проектирования систем управления 3.2. Методика проектирования функционального содержания управленческой деятельности 3.3. Методика проектирования организационной структуры системы управления	2	4		2	Изучить актуальные вопросы построения СЗИ	Письменная контрольная работа Практическое задание Лабораторная работа

	3.4. Методика оформления основных документов организационного проекта системы управления						
4	Структура и функции службы безопасности предприятия 4.1. Состав службы безопасности предприятия 4.2. Основные функции службы безопасности предприятия 4.3. Построение структурной схемы управления службой безопасности предприятия	2	4		2	Изучить вопросы оправданности построения СЗИ	Письменная контрольная работа Практическое задание Лабораторная работа
5	Подразделения службы безопасности предприятия 5.1. Подразделения режима и охраны 5.2. Специальный отдел 5.3. Подразделение информационно-аналитической деятельности 5.4. Подразделение инженерно-технической защиты 5.5. Подразделение разведки	2	4		2	Изучить зарубежный опыт подходов к оценке эффективности СЗИ	Письменная контрольная работа Практическое задание Лабораторная работа
6	Организация службы защиты информации 6.1. Создание СЗИ 6.2. Структура СЗИ 6.3. Организационно-технические мероприятия СЗИ 6.4. Руководитель службы защиты информации 6.5. Разработка должностных инструкций для специалистов по защите информации	2	4		2	Изучить советский опыт подходов к оценке эффективности СЗИ	Письменная контрольная работа Практическое задание Лабораторная работа
7	Управление службой безопасности предприятия (СБП) 7.1. Методы управления СБП 7.2. Функции процессов управления СБП 7.3. Принципы управления СБП 7.4. Обеспечение деятельности службы безопасности	2	4		2	Изучить российский опыт подходов к оценке эффективности СЗИ	Письменная контрольная работа Практическое задание Лабораторная работа

	7.5. Управление безопасностью предприятия в кризисных ситуациях					
8	<p>Подбор, расстановка и обучение сотрудников службы защиты информации</p> <p>8.1. Роль персонала в системе защиты информации 8.2. Набор и отбор персонала в СБП 8.3. Требования к специалистам по защите информации</p>	2	4		2	<p>Изучить правовые аспекты защиты информации в условиях чрезвычайных ситуаций. Оценить эффективность правовых аспектов защиты информации в условиях чрезвычайных ситуаций</p> <p>Письменная контрольная работа Практическое задание Лабораторная работа</p>
9	<p>Подбор, расстановка и обучение сотрудников службы защиты информации</p> <p>9.1. Организация обучения специалистов по защите информации 9.2. Требования к начальнику службы безопасности предприятия 9.3. Новые подходы к кадровому обеспечению службы информационной безопасности предприятия</p>	2	4		1	<p>Сравнить отечественный и зарубежный опыт подходов к оценке эффективности СЗИ</p> <p>Письменная контрольная работа Практическое задание Лабораторная работа</p>
	Итого	18	36		26	

