Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю
Руководитель ООП
Смирнова О.В.
«29» апреля 2024 г.

Рабочая программа дисциплины (с аннотацией)

«Информационная безопасность»

Направление подготовки
38.03.05 Бизнес-информатика

Профиль
«Бизнес-аналитика»

Для студентов 4 курса очной формы обучения
и 5 курса очно-заочной формы обучения

Составитель: Смирнова О.В., к.э.н., доцент

Тверь, 2024

I. Аннотация

1. Цель и задачи дисциплины

Целью освоения дисциплины является: формирование у обучающихся компетенций в области обеспечения информационной безопасности организаций и предприятий.

Задачами освоения дисциплины являются:

– знакомство с основными понятиями информационной безопасности, информационными угрозами, их классификацией, и возможными последствиями для организаций различных форм собственности;

– изучение вопросов обеспечения информационной безопасности организации и проблем создания систем информационной безопасности;

– принятие обоснованных решений по выбору политики информационной безопасности.

2. Место дисциплины в структуре ООП

Дисциплина «Информационная безопасность» относится к дисциплинам части, формируемой участниками образовательных отношений Блока 1 и направлена на формирование у обучающихся профессиональных компетенций.

Данная дисциплина логически и содержательно-методически связана с другими дисциплинами учебного плана, в частности, с дисциплинами «Информационные технологии и системы в экономике», «Информационно-аналитические системы управления предприятием», «Управление разработкой информационных систем» и др. Предпосылками для изучения дисциплины являются знания и умения, полученные в ходе освоения дисциплин «Информационные технологии и системы в экономике», «Информационно-аналитические системы управления предприятием», «Управление IT-инфраструктурой предприятия» и др. основной образовательной программы 38.03.05 Бизнес-информатика (профиль Бизнес-аналитика).

Освоение дисциплины «Информационная безопасность» является предшествующим при формировании компетенций для прохождения аналитической и преддипломной практик, предусмотренных учебным планом и выполнения ВКР.

3. Объем дисциплины: 3 зачетных единицы, 108 академических часов, **в том числе для очной формы обучения:**

контактная аудиторная работа: лекции 16 часов, практические занятия 16 часов.

самостоятельная работа: 76 часов.

в том числе для очно-заочной формы обучения:

контактная аудиторная работа: лекции 12 часов, практические занятия 12 часов.

самостоятельная работа: 84 часа.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ПК-1. Способен выполнять работы по созданию, модификации и сопровождению информационных систем для управления бизнес-процессами	ПК-1.4. Использует методы защиты информации в информационно-аналитических системах управления предприятием

5. Форма промежуточной аттестации и семестр прохождения:

по очной форме – зачет в 8 семестре;

по очно-заочной форме – зачет в 9 семестре.

6. Язык преподавания русский.

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

Для очной формы обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)					Самостоятельная работа, в том числе контроль (час.)
		Лекции		Практические занятия		Контроль самостоятельной работы (в том числе курсовая работа)	
		всего	в т.ч. практическая подготовка	всего	в т.ч. практическая подготовка		
Тема 1. Введение в информационную безопасность	27	4		4			19
Тема 2. Государственное регулирование информационной безопасности	27	4		4			19
Тема 3. Угрозы информационной безопасности.	27	4		4			19

Тема 4. Средства и методы обеспечения информационной безопасности	27	4		4			19
ИТОГО	108	16	0	16	0	0	76

Для очной-заочной формы обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)					Самостоятельная работа, в том числе Контроль (час.)
		Лекции		Практические занятия		Контроль самостоятельной работы (в том числе курсовая работа)	
		всего	в т.ч. практическая подготовка	всего	в т.ч. практическая подготовка		
Тема 1. Введение в информационную безопасность	25	2		2			21
Тема 2. Государственное регулирование информационной безопасности	25	2		2			21
Тема 3. Угрозы информационной безопасности.	29	4		4			21
Тема 4. Средства и методы обеспечения информационной безопасности	29	4		4			21
ИТОГО	108	12	0	12	0	0	84

Содержание разделов и тем по дисциплине

Тема 1. Введение в информационную безопасность

Информационная безопасность. Модели информационной безопасности. Виды защищаемой информации. Объекты и субъекты обеспечения информационной безопасности. Методы и средства обеспечения информационной безопасности. Системный подход к защите информации. Политика безопасности.

Тема 2. Государственное регулирование информационной безопасности

Правовой режим информационных ресурсов. Информационная безопасность в системе национальной безопасности Основные нормативно-правовые акты в области информационной безопасности РФ. Основы государственной политики РФ в области информационной безопасности.

Специальное законодательство в области информатизации информационных технологий и информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Приоритетные направления в области защиты информации в РФ. Стандарты информационной безопасности. Правовые нормы ИБ в организациях. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

Тема 3. Угрозы информационной безопасности

Информационные угрозы. Источники и предпосылки появления угроз. Характер происхождения угроз. Классификация угроз безопасности информации. Информационная атака. Несанкционированный доступ к защищаемой информации. Разглашение и утечка конфиденциальной информации. Способы воздействия угроз на информационные объекты. Идентификация угроз. Риски угроз информационным ресурсам.

Тема 4. Средства и методы обеспечения информационной безопасности

Функции и задачи защиты информации. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности. Стандарты информационной безопасности. Модели, стратегии и системы обеспечения информационной безопасности. Технические средства обеспечения защиты объекта: определение, системная классификация, общая характеристика. Инженерная защита объектов. Защита информации от утечки по техническим каналам. Программно-аппаратные средства обеспечения информационной безопасности. Обеспечение информационной безопасности операционных систем. Основы безопасности сетевых технологий. Средства и методы защиты от сетевых компьютерных угроз. Основы криптографической защиты информации. Сертификация и аттестация в области информационной безопасности.

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Тема 1. Введение в информационную безопасность	Лекции	Традиционная лекция, лекция-визуализация, дистанционные образовательные технологии
	Практические занятия	Групповая работа, решение практических заданий, дистанционные образовательные технологии
Тема 2. Государственное регулирование	Лекции	Традиционная лекция, лекция-визуализация, дистанционные образовательные технологии

информационной безопасности	Практические занятия	Групповая работа, решение практических заданий, кейсов, дистанционные образовательные технологии
Тема 3. Угрозы информационной безопасности	Лекции	Традиционная лекция, лекция-визуализация, дистанционные образовательные технологии
	Практические занятия	Групповая работа, решение практических заданий, кейсов, дистанционные образовательные технологии
Тема 4. Средства и методы обеспечения информационной безопасности	Лекции	Традиционная лекция, лекция-визуализация, дистанционные образовательные технологии
	Практические занятия	Групповая работа, решение практических заданий, дистанционные образовательные технологии

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения текущей аттестации

В связи с тем, что оценочные материалы должны обеспечивать возможность объективной оценки уровня сформированности компетенций, в рамках текущей аттестации включены: контрольные вопросы, тематика электронных презентаций, тематика письменных заданий, типовые case-study, типовые тесты, задачи и др.

Контрольные вопросы к практическим занятиям:

1. Охарактеризуйте правовые основы защиты конфиденциальной информации.
2. Охарактеризуйте организационные основы защиты конфиденциальной информации.
3. Определите основные виды угроз информационным ресурсам.
4. Охарактеризуйте технические каналы несанкционированного доступа к информации.
5. Дайте определение государственной тайны и назовите грифы секретности.
6. Каковы назначение, виды, структура и технология функционирования системы защиты информации?
7. Назовите направления и методы защиты служебной тайны.
8. Раскройте последовательность условия и формы допуска должностных лиц к государственной тайне.
9. Назовите причины, виды, каналы утечки и искажения информации.
10. Охарактеризуйте национальные интересы государства в информационной сфере.

Шкала оценки ответов на контрольные вопросы:

- Тема раскрыта с опорой на соответствующие понятия и теоретические положения и практику применения в организации – 2 балла.
- Терминологический аппарат не всегда (не полностью) связан с раскрываемой темой, практика применения малочисленна – 1 балл.
- Ответ свидетельствует о непонимании вопроса – 0 баллов.

Тематика электронных презентаций:

1. Виды угроз безопасности информации.
2. Методы несанкционированного доступа к информации.
3. Системный подход к защите информации.
4. Этапы проектирования системы защиты информации.
5. Особенности угроз автоматизированным информационным системам.
6. Направления и методы защиты служебной тайны.
7. Основные принципы управления рисками информационной безопасности.
8. Стандарты информационной безопасности.
9. Компьютерные преступления.
10. Ущерб от компьютерных злоупотреблений.

* обучающимися могут быть предложены другие темы электронных презентаций по согласованию с преподавателем.

Шкала оценки презентаций:

- Тема раскрыта с опорой на соответствующие понятия и теоретические положения, презентация полностью соответствует требованиям – 2 балла.
- Терминологический аппарат непосредственно слабо связан с раскрываемой темой, имеются недостатки в составлении и оформлении презентации – 1 балл.
- Допущены фактические и логические ошибки, свидетельствующие о непонимании темы, имеются недостатки в составлении и оформлении презентации – 0 баллов.

Типовые практические задания:

Задание 1. Составьте фрагмент номенклатуры дел, содержащих конфиденциальные документы.

Задание 2. Составьте и проанализируйте технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.

Задание 3. Составьте схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализируйте степень опасности каждого канала.

Шкала оценки практического задания:

- Ответ полностью соответствует условиям задания и обоснован – 2 балла.
- Ответ в целом соответствует условиям задания, но отдельные аспекты на обоснованы (или обоснованы частично) – 1 балл.
- Ответ частично соответствует условиям задания, отдельные аспекты не обоснованы или имеются существенные ошибки – 0 баллов.

Типовые кейсы

Вы – сотрудник отдела информационной безопасности предприятия. Подготовьте отчет для руководителя отдела, включающий в себя следующие задания:

1) Подготовьте аналитику за последние 2 года с описанием 10-ти самых опасных вредоносных программ именно для ИТ-инфраструктуры.

2) Приведите примеры, каким образом угрозы повлияли на крупнейшие компании (пострадавшие) и на индустрию защиты данных в целом.

3) Подберите программные (аппаратные) решения для следующих уровней защиты (по 1 на уровень) и кратко опишите их функциональные возможности:

- сеть передачи данных (файервол, VPN для внешнего подключения);
- рабочий ПК сотрудника (антивирусное ПО);
- хранения данных (программный бекап);
- сервер электронной почты (антиспам, бекап и восстановление Exchange);
- Active Directory (восстановление доступа сотрудников);
- виртуальные машины (High availability);
- доступ в офис (электронные магнитные карты HID).

Шкала оценки выполнения кейсов:

- Ответ полностью соответствует условиям задания и обоснован – 2 балла.
- Ответ в целом соответствует условиям задания, но отдельные аспекты на обоснованы – 1 балл.
- Ответ частично соответствует условиям задания, отдельные аспекты не обоснованы или имеются несущественные ошибки – 0 баллов.

Пример типовых тестов

1. Политика безопасности – это:

а) пошаговые инструкции по выполнению задач безопасности;

б) общие руководящие требования по достижению определенного уровня безопасности;

в) широкие, высокоуровневые заявления руководства;

г) детализированные документы по обработке инцидентов безопасности.

2. Что лучше всего описывает цель расчета ALE:

а) количественно оценить уровень безопасности среды;

б) оценить возможные потери для каждой контрмеры;

в) количественно оценить затраты / выгоды;

г) оценить потенциальные потери от угрозы в год.

3. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой:

а) анализ связующего дерева;

б) AS/NZS;

в) NIST;

г) анализ сбоев и дефектов.

4. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

а) гаммирования;

б) подстановки;

в) кодирования;

г) перестановки;

д) аналитических преобразований.

5. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

а) черный пиар;

б) фишинг;

в) нигерийские письма;

г) источник слухов;

д) пустые письма.

6. На каком уровне защиты информации находятся непосредственно средства защиты:

а) законодательный;

б) процедурный;

в) программно-технический;

г) административный.

7. Как называется государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных:

а) субъект персональных данных;

б) оператор информационной системы;

в) регулятор;

г) оператор персональных данных.

8. Какая из ниже приведенных методик внедрения системы защиты против инсайдеров соответствует цели выявления канала утечки?

а) открытое внедрение в сочетании с кадровой работой;

б) внедрение контролей, проверяемых при аудите;

в) скрытое внедрение в сочетании с ОРМ;

г) архивация движения данных и сетевых операций для доказательства того, что источник утечки не внутри фирмы.

9. Заключительным этапом построения системы защиты является:

а) сопровождение;

б) планирование;

в) анализ уязвимых мест;

г) нет верного ответа.

10. Принципом политики информационной безопасности является принцип:

а) разделения доступа (обязанностей, привилегий) клиентам сети (системы)

б) одноуровневой защиты сети, системы;

в) совместимых, однотипных программно-технических средств сети, системы;

г) перехода в безопасное состояние работы сети, системы.

Шкала оценки тестов:

- 75% правильных ответов – 2 балла.
- 65% правильных ответов – 1 балл.
- 64% и менее правильных ответов – 0 баллов.

Оценочные материалы для проведения промежуточной аттестации

Планируемые результаты по ПК-1 – Способен выполнять работы по созданию, модификации и сопровождению информационных систем для управления бизнес-процессами:

ПК-1.4. Использует методы защиты информации в информационно-аналитических системах управления предприятием.

Пример типового комплексного задания
для проведения промежуточной аттестации

Структура комплексного задания:

Задание 1 – теоретико-практическое: обоснование ответа на поставленные вопросы с приведением практических примеров.

Задание 2 – практическое задание.

Примерные вопросы теоретико-практической направленности

1. Национальная безопасность и её составляющие.
2. Базовые требования безопасности компьютерной системы.
3. Классы средств защиты информации.
4. Методы и средства обеспечения ИБ объектов информационной сферы.
5. Методы нарушения конфиденциальности, целостности и доступности информации.

Типовые практические задания

1. Проанализируйте пути поиска документов и дел, не обнаруженных при проверке их наличия, дайте возможные рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.

2. Составьте и проанализируйте технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией.

Шкала оценки степени сформированности компетенций обучающихся на промежуточной аттестации в рамках рейтинговой системы *(по очной форме обучения)*

Контрольное задание на зачете	Индикаторы	Количество рейтинговых баллов
Часть 1	ПК-1.4. Использует методы защиты информации в информационно-аналитических системах управления предприятием	10
Часть 2	ПК-1.4. Использует методы защиты информации в информационно-аналитических системах управления предприятием	30
Итого		40

Шкала оценивания соотнесена с рейтинговыми баллами.

В соответствии с «Положением о рейтинговой системе обучения в ТвГУ», утвержденным врио ректора от 29.06.2022 г., максимальная сумма баллов по учебной дисциплине, заканчивающейся зачетом, по итогам семестра составляет 100 баллов. Обучающемуся, набравшему 40 баллов и выше по итогам работы в семестре выставляется оценка «зачтено». Обучающийся, набравший до 39 баллов включительно, сдает зачет.

Шкала оценки степени сформированности компетенций обучающихся на промежуточной аттестации по *(по очно-заочной обучения)*

Контрольное задание на зачет	Оценка «не зачтено	Оценка «зачтено»
Часть 1	При ответе на теоретические вопросы допущены неточности, практические задания не выполнены; при ответе на теоретические вопросы допущены существенные неточности, практические задания выполнены не в полном объеме.	Даны полные и правильные ответы на теоретические вопросы, практические задания выполнены правильно.
Часть 2		

Форма проведения промежуточной аттестации: устная или письменная.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

1) Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642.
2) Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2024. — 325 с. — (Высшее образование). — Текст : электронный. — URL: https://urait.ru/bcode/536225.
3) Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — Текст : электронный— URL: https://urait.ru/bcode/544029
4) Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1912987.

б) Дополнительная литература

1) Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — Текст : электронный — URL: https://urait.ru/bcode/544290.
2) Козырь, Н. С. Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва : Издательство Юрайт, 2024. — 131 с. — (Высшее образование). — Текст : электронный. — URL: https://urait.ru/bcode/545066.
3) Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2024. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - Текст : электронный. - URL: https://znanium.com/catalog/product/2052391.
4) Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 327 с. — (Высшее образование). — Текст : электронный — URL: https://urait.ru/bcode/542739.
5) Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022.

2) Лицензионное программное обеспечение и свободно распространяемое программное обеспечение, в т.ч. отечественного производства

а) Лицензионное программное обеспечение

2-ая Грибоедова, д.22, корпус 7, аудитории 105, 106

Список ПО	Условия предоставления
Adobe Reader XI (11.0.13) - Russian	бесплатно

Google Chrome	бесплатно
Audit XP	Акт предоставления прав № Tr063036 от 11.11.2014
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Project Expert 7 Tutorial	Договор №40 от 11.09.2012.
Audit Expert 7 Tutorial	Договор №40 от 11.09.2012.
Prime Expert 7 Tutorial	Договор №40 от 11.09.2012.
CorelDRAW Graphics Suite X4 Education License	Акт приема- передачи № Tr034515 от 15.12.2009
AnyLogic PLE	бесплатно
iTALC	бесплатно
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

2-ая Грибоедова, д.22, корпус 7, аудитория 107

Список ПО	Условия предоставления
Adobe Reader XI (11.0.13) - Russian	бесплатно
Google Chrome	бесплатно
1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях.	Акт приема-передачи №Tr034562 от 15.12.2009
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
СПС ГАРАНТ аэро	договор №5/2018 от 31.01.2018
Консультант +	договор № 2018С8702
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

б) Свободно распространяемое программное обеспечение

Google Chrome	бесплатное ПО
Яндекс Браузер	бесплатное ПО
Kaspersky Endpoint Security 10	акт на передачу прав ПК545 от 16.12.2022
Многофункциональный редактор ONLYOFFICE	бесплатное ПО
ОС Linux Ubuntu	бесплатное ПО

- и др.

3) Современные профессиональные базы данных и информационные справочные системы:

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.
2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.

3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.
4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.
5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.
6. Научная электронная библиотека eLIBRARY.RU (подписка на журналы): https://elibrary.ru/projects/subscription/rus_titles_open.asp?
7. Репозитарий ТвГУ http://eprints.tversu.ru

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. СПС КонсультантПлюс (в сети ТвГУ)
2. Официальный интернет-портал правовой информации http://pravo.gov.ru/
3. Сводные каталоги фондов российских библиотек АРБИКОН, МАРС https://mars.arbicon.ru/index.php, http://corbis.tverlib.ru/catalog/
4. Федеральный образовательный портал «Экономика Социология Менеджмент» http://ecsocman.hse.ru
5. Polpred.com Обзор СМИ http://www.polpred.com/
6. База данных «Финансовая математика – Библиотека управления» - Корпоративный менеджмент https://www.cfin.ru/finanalysis/math/

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации по подготовке к лекционным, практическим занятиям и по организации самостоятельной работы

Самостоятельная работа начинается до прихода студента на лекцию. Целесообразно использование «системы опережающего чтения», т.е. предварительного прочтения лекционного материала, содержащегося в учебниках и учебных пособиях, закладывающего базу для более глубокого восприятия лекции. Работа над лекционным материалом включает два основных этапа: конспектирование лекций и последующую работу над лекционным материалом. Под конспектированием подразумевают составление конспекта, т.е. краткого письменного изложения содержания чего-либо (устного выступления – речи, лекции, доклада и т.п. или письменного источника – документа, статьи, книги и т.п.).

Методика работы при конспектировании устных выступлений значительно отличается от методики работы при конспектировании письменных источников. Конспектируя письменные источники, студент имеет возможность неоднократно прочитать нужный отрывок текста, поразмыслить над ним, выделить основные мысли автора, кратко сформулировать их, а затем записать. При необходимости он может отметить и свое отношение к этой точке зрения. Слушая же лекцию, студент большую часть комплекса указанных выше работ должен откладывать на другое время,

стремясь использовать каждую минуту на запись лекции, а не на ее осмысление – для этого уже не остается времени. Поэтому при конспектировании лекции рекомендуется на каждой странице отделять поля для последующих записей в дополнение к конспекту.

Записав лекцию или составив ее конспект, не следует оставлять работу над лекционным материалом до начала подготовки к зачету. Нужно проделать как можно раньше ту работу, которая сопровождает конспектирование письменных источников и которую не удалось сделать во время записи лекции: прочесть свои записи, расшифровав отдельные сокращения, проанализировать текст, установить логические связи между его элементами, в ряде случаев показать их графически, выделить главные мысли, отметить вопросы, требующие дополнительной обработки, в частности, консультации преподавателя. При работе над текстом лекции студенту необходимо обратить особое внимание на проблемные вопросы, поставленные преподавателем при чтении лекции, а также на его задания и рекомендации.

Перечень вопросов, подлежащих изучению, приведен в данной рабочей программе дисциплины (контрольные вопросы для проведения текущей аттестации; вопросы для подготовки к зачету). Не все эти вопросы будут достаточно полно раскрыты на лекциях. Отдельные вопросы будут освещены недостаточно полно или вообще не будут затронуты. Поэтому, проработав лекцию по конспекту, необходимо сравнить перечень поднятых в ней вопросов с тем перечнем, который приведен в рабочей программе дисциплины (контрольные вопросы для проведения текущей аттестации; вопросы для подготовки к зачету), и изучить ряд вопросов по учебным пособиям, дополняя при этом конспект лекций.

Студентам заочной формы обучения необходимо обратить внимание на то, что как видно из п. II «Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий» (для очно-заочной формы обучения), на сессии будут прочитаны лекции не по всем темам курса. Часть тем будет вынесена на самостоятельное изучение студентами, прежде всего с помощью учебных пособий. Следует помнить, что работа с учебными пособиями не имеет ничего общего со сквозным пограничным чтением текста. Она должна быть направлена на поиски ответов на конкретно поставленные вопросы (контрольные вопросы для проведения текущей аттестации; вопросы для подготовки к экзамену). Работая с учебными пособиями, не следует забывать о справочных изданиях.

При работе над темами, которые вынесены на самостоятельное изучение, студент должен самостоятельно выделить наиболее важные, узловые проблемы, как это в других темах делалось преподавателем. Здесь не следует с целью экономии времени подходить к работе поверхностно, ибо в таком случае повышается опасность «утонуть» в обилии материала, упустить центральные проблемы. Результатом самостоятельной работы должно стать собственное самостоятельное представление студента об изученных вопросах.

Самостоятельная работа по изучению тем дисциплины по учебным пособиям не должна состоять из сквозного чтения или просмотра текста. Она должна включать вначале ознакомительное чтение, а затем поиск ответов на конкретные вопросы. Основная трудность для студентов заключается здесь в необходимости усвоения, понимания и запоминания значительных объемов материала. Эту трудность, связанную, прежде всего, с дефицитом времени, можно преодолеть путем усвоения интегрального алгоритма чтения.

При подготовке к практическим занятиям следует закрепить полученные теоретические знания по теме и получить практические навыки в их применении путем рассмотрения примеров решения задач по изучаемой теме, рассмотренных в рекомендованной литературе.

В процессе самостоятельной работы большое значение имеют консультации с преподавателем, в ходе которых можно решить многие проблемы изучаемой дисциплины, уяснить сложные вопросы. При возникновении трудностей в изучении каких-либо вопросов целесообразно попытаться уяснить их, воспользовавшись другим рекомендованным учебным пособием. Если изучение непонятого материала по другому учебному пособию не привело к его усвоению, то следует обратиться за консультацией к преподавателю данной дисциплины.

Методические рекомендации по организации самостоятельной работы обучающихся

Для качественной организации самостоятельной работы обучающихся преподаватель должен:

– овладеть технологией диагностики умений и навыков самостоятельной работы обучающихся в целях соблюдения преемственности в их совершенствовании;

– продумать процесс поэтапного усложнения заданий для самостоятельной работы обучающихся;

– обеспечить самостоятельную работу обучающихся учебно-методическими материалами, отвечающими современным требованиям управления указанным видом деятельности;

– разработать систему контрольно-измерительных материалов, призванных выявить уровень знаний.

Методические рекомендации по подготовке к промежуточной аттестации

Зачет – важный этап в учебном процессе, имеющий целью проверку знаний, выявление умений применять полученные знания к решению практических задач. Как подготовка к зачету, так и сам зачет - форма активизации и систематизации полученных знаний, их углубления и закрепления. Подготовка к зачету для студентов, особенно заочной формы обучения, всегда осложняется дефицитом времени.

Для подготовки к зачету необходимо:

1) ознакомиться с перечнем вопросов для подготовки к зачету (а также с контрольными вопросами для проведения текущей аттестации) и при необходимости повторить их с использованием конспекта лекций и / или рекомендованных учебных пособий;

2) повторить решение типовых задач, приведенных в п. IV «Оценочные средств для проведения текущей и промежуточной аттестации» (типовые задачи для проведения текущей аттестации; примерные задания для проведения промежуточной аттестации), а также решение задач, задаваемых преподавателем для самостоятельного выполнения по рекомендованным учебным пособиям;

3) при возникновении каких-либо вопросов, трудностей в уяснении теоретического материала или проблем с решением задач прибегнуть к помощи Вашего преподавателя и / или других студентов Вашей группы.

Вопросы для самоподготовки:

1. Основные нормативные правовые акты, определяющие концептуальные основы информационной безопасности РФ.
2. Информационное право и информационная безопасность.
3. Содержание концепции национальной безопасности РФ.
4. Причины и источники угроз национальным интересам страны.
5. Информационная война, методы и средства её ведения.
6. Методы нарушения конфиденциальности, целостности и доступности информации.
7. Причины, виды, каналы утечки и искажения информации.
8. Угрозы и их классификация.
9. Основные угрозы конфиденциальности.
10. Вредоносное программное обеспечение.
11. Основные направления обеспечения информационной безопасности объектов информационной сферы.
12. Методы и средства обеспечения информационной безопасности объектов информационной сферы.
13. Стандарты обеспечения информационной безопасности.
14. Электронный документ, электронная цифровая подпись, владелец сертификата ключа подписи, средства электронной цифровой подписи, сертификат средств электронной цифровой подписи.
15. Архивное хранение конфиденциальных документов.
16. Направления и методы защиты документов на бумажных носителях.
17. Построение и функционирование защищенного документооборота.
18. Оценочные стандарты и технические спецификации.
19. Базовые требования безопасности компьютерной системы.
20. Классы безопасности компьютерных систем, понятие риска.
21. Сетевые механизмы безопасности.
22. Направления и методы защиты служебной тайны.
23. Направления и методы защиты персональных данных граждан.

24. Экономические основы защиты конфиденциальной информации.
25. Организационные основы защиты конфиденциальной информации.

Методические рекомендации по подготовке электронных презентаций

Подготовка электронных презентаций состоит из следующих этапов:

1. Планирование презентации: определение основных содержательных аспектов доклада: определение целей; определение основной идеи презентации; подбор дополнительной информации; создание структуры презентации; проверка логики подачи материала; подготовка заключения.

2. Разработка презентации – подготовка слайдов презентации, включая вертикальную и горизонтальную логику, содержание и соотношение текстовой и графической информации в соответствии с требованиями.

Требования к мультимедийной презентации

Требования к структуре	• Количество слайдов адекватно количеству представленной информации; • наличие титульного слайда; • наличие слайда с использованными источниками.
Требования к содержанию	• Отражение в презентации основных этапов исследования (проблемы, цели, гипотезы, хода работы, выводов); • содержание ценной, полной, понятной информации по теме; • отсутствие грамматических ошибок и опечаток.
Требования к тексту	• Текст на слайде представляет собой опорный конспект (ключевые слова, маркированный или нумерованный список), без полных предложений; • выделение наиболее важной информации с помощью цвета, размера, эффектов анимации.
Требования к шрифту	• Использование шрифта для заголовков не менее кегля 24, для информации – не менее кегля 18; • использование строчных букв.
Требования к средствам наглядности	• Использование средств наглядности информации (таблицы, схемы, графики и т.д.); • использование иллюстраций хорошего качества, с четким изображением; • использование иллюстраций, помогающих наиболее полно раскрыть тему, не отвлекая от содержания.
Требования к оформлению	• Соответствие стиля оформления презентации (графического, звукового, анимационного) теме и содержанию выступления; • Использование единого стиля оформления для всех слайдов презентации; • оправданное использование эффектов.

Требования к рейтинг-контролю

Рейтинговый контроль знаний осуществляется в соответствии с *Положением о рейтинговой системе обучения в ТвГУ, утвержденным ученым советом ТвГУ 29.06.2022 г., протокол №11*.

Распределение баллов по видам работы в рамках рейтинговой системы:

Вид отчетности	Баллы
Работа в семестре, в том числе: текущий контроль рейтинговый контроль	100 60 40
Зачет	по факту
Итого:	100

VII. Материально-техническое обеспечение

Материально-техническая база необходимая и применяемая для осуществления образовательного процесса и программное обеспечение по дисциплине включает (в соответствии с паспортом аудитории):

– специальные помещения (аудитории), укомплектованные специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации в аудитории;

– мультимедийное оборудование (ноутбук, экран и проектор);

– ПК для работы студентов в компьютерном классе с выходом в Интернет.

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	Обновленный раздел рабочей программы дисциплины	Описание внесенных изменений	Реквизиты документа, утвердившего изменения
1.			
2.			