Автономная некоммерческая образовательная организация высшего образования
«Сибирский институт бизнеса и информационных технологий»

«УТВЕРЖДАЮ»
Ректор
_____ М.Г. Родионов
19 февраля 2020 г.

Рабочая программа дисциплины
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

образовательной программы профессиональной переподготовки
«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ»

Квалификация выпускника
«Специалист в области информационных технологий в управлении»

Форма обучения
заочная, в т.ч. с применением ДОТ

Омск – 2020

Рабочая программа дисциплины «Информационная безопасность» образовательной программы профессиональной переподготовки (далее ОППП) «Информационные технологии в управлении».

Автор:

старший преподаватель факультета
очного обучения СИБИТ, к.э.н. _____ Е.В.Куликова
(подпись)

Рецензент:
Заместитель начальника Главного управления
информационных технологий и связи Омской области _____ А.А. Ключенко
(подпись)

Программа одобрена Научно-методическим советом института.

Протокол № 5 от 19.02.2020 г.

Председатель НМС,
доцент факультета очного обучения, _____ С.П. Вольф
кандидат исторических наук (подпись)

При разработке рабочей программы дисциплины «Информационная безопасность» подготовки слушателя по программе «Информационные технологии в управлении» Институт руководствовался:

1. Конституцией Российской Федерации;
2. Федеральным законом «Об образовании в Российской Федерации» от 29 декабря 2012 г. № 273- ФЗ;
3. Приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
4. Квалификационным справочником должностей руководителей, специалистов и других служащих, утвержденного постановлением Минтруда РФ от 21 августа 1998 г. № 37;
5. Приказом Минтруда России от 12 апреля 2013 г. № 148 н «Об утверждении уровней квалификаций в целях разработки проектов профессиональных стандартов»;
6. Методическими рекомендациями по разработке дополнительных профессиональных программ на основе профессиональных стандартов (письмо Минобрнауки России от 22 апреля 2015 года № ВК-1032/06);
7. Методическими рекомендациями по реализации дополнительных профессиональных программ с использованием дистанционных образовательных

технологий, электронного обучения и в сетевой форме (письмо Минобрнауки России от 21 апреля 2015 года № ВК-1013/06);

8. Методическими рекомендациями по итоговой аттестации слушателей (письмо Минобрнауки России от 30 марта 2015 года № АК-820/06).

9. Уставом «Сибирского института бизнеса и информационных технологий»;

10. Положением о центре дополнительного образования и иными локальными актами института.

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОППП

Цель дисциплины «Информационная безопасность» - изучить основные понятия информационной безопасности, основы построения систем защиты информации программным, техническим и организационно-правовым обеспечением.

Задачи дисциплины:

- усвоение теоретических основ методологии информационной безопасности;
- овладение методами, используемыми в процессе защиты информации;
- формирование представлений о логике и технологии информационной безопасности;
- изучение организационных мероприятий, связанных с защитой информации;
- приобретение навыков защиты информации от несанкционированного доступа;
- усвоение теоретических и практических навыков организации защиты информации в компьютерных системах и сетях;
- получение базовых представлений о методах и средствах защиты локальных и корпоративных сетей от удаленных атак через сеть Internet.

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

Коды компетенций	Название компетенции	Перечень планируемых результатов обучения по дисциплине
1	2	3
	ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ ВЫПУСКНИКА	
ПК-3	Принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	**Знать:** – виды угроз информационной безопасности; – методы управления информационной безопасностью предприятия; – устройство и функционирование современных ИС, отвечающих требованиям информационной безопасности. **Уметь:** – устанавливать и настраивать системное и прикладное ПО, необходимое для обеспечения информационной безопасности ИС; – идентифицировать основные угрозы информационной безопасности и принимать участие в их ликвидации. **Владеть:** – методами обследования и организации ИТ-инфраструктуры организации; – методами и средствами оптимизации ИТ-инфраструктуры предприятия с учетом обеспечения информационной безопасности; - средствами, методами и инструментами управления информационной безопасностью предприятия и электронного бизнеса.

Планируемые результаты освоения дисциплины соотнесены с профессиональными задачами, описанными в ФГОС ВО, и трудовыми функциями, содержащимися в профессиональных стандартах:

проектная деятельность: –формирование требований к информатизации и автоматизации прикладных процессов; **организационно-управленческая деятельность:** –участие в организации и управлении информационными ресурсами и сервисами.	Принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-3)	**B/17.5** Установка и настройка системного и прикладного ПО, необходимого для функционирования ИС	–устанавливать и настраивать системное и прикладное ПО, необходимое для обеспечения информационной безопасности ИС; –идентифицировать основные угрозы информационной безопасности и принимать участи в их ликвидации.	–виды угроз информационной безопасности в ИС; –методы управления информационной безопасностью предприятия; –основы управления информационной безопасностью; –устройство и функционирование современных ИС, отвечающих требованиям информационной безопасности;

2. Объем дисциплины в академических часах и вид промежуточной аттестации

Общая трудоемкость дисциплины составляет 22 часа.
Вид промежуточной аттестации – зачет.

Виды учебных занятий	Всего часов
Общая трудоемкость дисциплины	**22**
лекции	2
лабораторные работы	-
практические занятия	2
Самостоятельная работа слушателя	**18**

3. Содержание дисциплины, структурированное по темам

3.1. Темы дисциплины и трудоемкость по видам учебных занятий в часах

Формируемые компетенции	Раздел/тема дисциплины, содержание	ВСЕГО	Всего	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа, всего
ПК -3	1. Общие проблемы информационной безопасности. Роль и место информационной безопасности	**3**	**1**	1			**2**
	2. Понятие организационной защиты информации	**3**	**1**			1	**2**
	3. Связь и информатизация	**3**	**1**			1	**2**
	4. Криптографические методы защиты информации	**4**	**1**	1			**3**
	5. Защита информации в персональных компьютерах	**2**					**2**
	6. Экономическая безопасность	**2**					**2**
	7. Проблемы защиты информации в сетях электронно-вычислительных машин	**2**					**2**
	8. Технические средства и комплексное обеспечение безопасности	**3**					**3**
	ВСЕГО	**22**	**4**	2		2	**18**

Форма промежуточной аттестации – зачет. Зачет проводится в виде тестирования.

3.2. Содержание дисциплины, структурированное по темам

ТЕМА 1. ОБЩИЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭКОНОМИКЕ И УПРАВЛЕНИИ НАРОДНЫМ ХОЗЯЙСТВОМ. РОЛЬ И МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Национальные интересы и безопасность. Уровни обеспечения национальной безопасности. Группы субъектов уровней в системе национальной безопасности.

Экономические отношения, возникающие в процессе развития народного хозяйства; методы, механизмы, инструменты и технологии функционирования экономических систем и институциональных преобразований в условиях рыночной экономики с учетом тенденций глобализации экономических процессов в отраслях промышленности.

Принципы, задачи и функции обеспечения информационной безопасности в в экономике и управлении народным хозяйством.

Вопросы для обсуждения:

1) Принципы обеспечения информационной безопасности.
2) Задачи обеспечения информационной безопасности.
3) Функции обеспечения информационной безопасности.

Тема 2. Понятие организационной защиты информации.

Введение в организационное обеспечение информационной безопасности. Сущность организационных методов защиты информации. Соотношение организационных мер защиты информации с мерами правового и технического характера. Основные термины, связанные с организацией защиты информации.

Предметные направления защиты информации: государственная, коммерческая, банковская, профессиональная, служебная тайны, охрана персональных данных, охрана интеллектуальной собственности.

Виды доступа к информации. Виды отношений между субъектами по степени ограничения доступа.

Правовые основы защиты информации.

Вопросы для обсуждения:

1) Конституционные гарантии.
2) Защита прав собственности на информацию.
3) Уровни доступа к информации с точки зрения законодательства.
4) Информация без ограничения права доступа.
5) Информация с ограниченным доступом.
6) Информация, распространение которой наносит вред интересам общества.
7) Объекты интеллектуальной собственности.

Тема 3. Связь и информатизация

Явления и процессы, свойственные связи и информатизации как специфической отрасли человеческой деятельности; производственные отношения в сфере связи и информатизации; закономерности функционирования, планирования, управления и развития предприятий отрасли и их влияние на другие сферы человеческой деятельности.

Угрозы информации в автоматизированных системах связи и информатизации.

Вопросы для обсуждения:

1) Каналы несанкционированного получения информации в системах связи и информатизации.
2) Понятие угрозы информации в системах связи и информатизации.
3) Оценка угроз.
4) Преднамеренные угрозы безопасности систем связи и информатизации.
5) Признаки угроз безопасности и их классификация.

Тема 4. Криптографические методы защиты информации.

Основные этапы развития криптологии. Основные понятия криптологии. Требования к криптографическим системам. Классификация методов криптографического закрытия. Симметричные криптосистемы.

1) Шифрование заменой (подстановкой).
2) Прямая замена.
3) Полиалфавитные подстановки.
4) Таблица Вижинера.

Тема 5. Защита информации в персональных компьютерах.

Особенности защиты информации в персональных компьютерах. Факторы, влияющие на определение целесообразного выбора подхода к защите информации в персональных компьютерах.

Основные цели защиты информации. Угрозы информации в персональных компьютерах. Обеспечение целостности информации в персональных компьютерах. Актуальность данного вида защиты. Угрозы целостности информации в персональных компьютерах. Защита персонального компьютера от несанкционированного доступа. Основные механизмы защиты персонального компьютера от несанкционированного доступа. Физическая защита персонального компьютера и носителей информации.

Опознавание (аутентификация) пользователей и используемых компонентов обработки информации. Способы опознавания пользователей.

Разграничение доступа к элементам защищаемой информации.

Криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных).

Тема 6. Экономическая безопасность

Проблемы экономической безопасности открытых национальных экономических систем. Понятия и показатели экономической безопасности национальной экономики. Содержание концепции и стратегии экономической безопасности России. Пороговые значения показателей экономической безопасности национальной экономики. Интегральный и частный критерий экономической безопасности.

Тема 7. Проблемы защиты информации в сетях электронно-вычислительных машин.

Цели, функции и задачи защиты информации в сетях электронно-вычислительных машин. Особенности защиты информации в вычислительных сетях.

Понятие и особенности сервиса безопасности электронно-вычислительных сетей. Идентификация и аутентификация. Условия идентификации и аутентификации. Разграничение доступа. Протоколирование (аудит). Экранирование. Функции экранирования. Межсетевые экраны. Туннелирование. Шифрование. Понятие и особенности контроля целостности. Понятие и особенности контроля защищенности. Обнаружение отказов и оперативное восстановление. Процесс администрирования.

Тема 8. Технические средства и комплексное обеспечение безопасности.

Понятие комплексного подхода к обеспечению безопасности. Система физической безопасности и её подсистемы. Средства противодействия.

Понятие технических средств. Достоинства технических средств. Недостатки технических средств. Классификация технических средств. Критерии сопряженности с основными средствами автоматизированных систем обработки данных. Критерии выполняемой функции защиты. Степени сложности устройства.

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

4.1. Виды и организация самостоятельной работы обучающихся

Успешное освоение теоретического материала по дисциплине «Информационная безопасность» требует ***самостоятельной работы***, нацеленной на усвоение лекционного теоретического материала, расширение и конкретизацию знаний по разнообразным вопросам обеспечения исполнения обязательств. Самостоятельная работа слушателей может быть аудиторной, внеаудиторной, а также проводиться в электронной информационно-образовательной среде.

1. *Аудиторная самостоятельная работа слушателей* – выполнение на семинарских занятиях заданий, закрепляющих полученные теоретические знания либо расширяющие их, а также выполнение разнообразных контрольных заданий индивидуального или группового характера (подготовка устных докладов или сообщений о результатах выполнения заданий, выполнение самостоятельных проверочных работ по итогам изучения отдельных вопросов и тем дисциплины);

2. *Внеаудиторная самостоятельная работа слушателей* – подготовка к лекционным и семинарским занятиям, повторение и закрепление ранее изученного теоретического материала, конспектирование учебных пособий и периодических изданий, изучение проблем, не выносимых на лекции, написание тематических рефератов, эссе, выполнение практических заданий, подготовка к тестированию по дисциплине.

Большое значение в преподавании дисциплины отводится самостоятельному поиску слушателями информации по отдельным теоретическим и практическим вопросам и проблемам.

Наиболее целесообразен следующий порядок изучения теоретических вопросов по дисциплине «Информационная безопасность»:

1. Изучение справочников (словарей, энциклопедий) с целью уяснения значения основных терминов, понятий, определений;

2. Изучение учебно-методических материалов для лекционных и семинарских занятий;

3. Изучение рекомендуемой основной и дополнительной литературы и электронных информационных источников;

4. Изучение дополнительной литературы и электронных информационных источников, определенных в результате самостоятельного поиска информации;

5. Самостоятельная проверка степени усвоения знаний по контрольным вопросам и/или заданиям;

6. Повторное и дополнительное (углубленное) изучение рассмотренного вопроса (при необходимости).

В процессе самостоятельной работы над учебным материалом рекомендуется составить конспект, где кратко записать основные положения изучаемой темы. Переходить к следующему разделу можно после того, когда предшествующий материал понят и усвоен. В затруднительных случаях, встречающихся при изучении курса, необходимо обратиться за консультацией к преподавателю.

При изучении дисциплины не рекомендуется использовать материалы, подготовленные неизвестными авторами, размещенные на неофициальных сайтах неделового содержания. Желательно, чтобы используемые библиографические источники были изданы в последние 3-5 лет. Слушатели при выполнении самостоятельной работы могут воспользоваться учебно-методическими материалами по дисциплине «Информационная безопасность», представленными в электронной библиотеке института, и предназначенными для подготовки к лекционным и семинарским занятиям.

Перечень основных учебно-методических материалов для лекционных и семинарских занятий представлен в п. 7. рабочей программы дисциплины.

Контроль аудиторной самостоятельной работы осуществляется в форме дискуссии, собеседования. Контроль внеаудиторной самостоятельной работы слушателей осуществляется в форме устного или письменного опроса.

Промежуточный контроль знаний в форме зачета осуществляется посредством письменного тестирования, включающего вопросы и задания для самостоятельного изучения.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ СЛУШАТЕЛЕЙ ПО ДИСЦИПЛИНЕ

5.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОППП

Освоение дисциплины направлено на формирование:

профессиональных компетенций:

- способностью соблюдения законодательства РФ (ПК-3);

Данные компетенции формируются в процессе изучения дисциплины на этапе промежуточной аттестации.

5.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Промежуточная аттестация по дисциплине проводится в форме зачета в виде тестирования.

Тестовые задания разрабатываются по основным вопросам теоретического материала и позволяют осуществлять промежуточный контроль знаний и степени усвоения материала.

При проведении промежуточной аттестации слушателей по дисциплине «Информационная безопасность» формируются варианты тестов, относящихся ко всем темам дисциплины.

Оценка знаний слушателей осуществляется в соответствии с технологической картой дисциплины.

№ п/п	Показатели оценивания	Критерии оценивания	Шкала оценивания
1	Тестирование	Количество баллов за тест пропорционально количеству правильных ответов на тестовые задания. После прохождения теста суммируются результаты выполнения всех заданий для выставления общей оценки за тест.	0-100

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

5.3.1. Типовые контрольные задания или иные материалы на этапе промежуточной аттестации

Тестовые задания (25 вопросов)

1. Из следующих утверждений выберите одно неверное

а) Термин «компьютерная безопасность» можно употреблять как заменитель термина «информационная безопасность»
б) Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности
в) Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации

2. Составляющими информационной безопасности являются

а) обеспечение доступности, целостности
б) обеспечение доступности, целостности, конфиденциальности информационных ресурсов и поддерживающей инфраструктуры
в) обеспечение доступности, конфиденциальности информационных ресурсов и поддерживающей инфраструктуры

3. Возможность за приемлемое время получить требуемую информационную услугу – это составляющая информационной безопасности:

а) Доступность
б) Целостность
в) Конфиденциальность

4. По области регламентации выделяют следующие виды стандартов:

а) Международные и национальные
б) Оценочные и спецификации
в) Обязательные и рекомендуемые
г) Общедоступные и распространяемые по лицензии

5. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения – это составляющая информационной безопасности

а) Доступность
б) Целостность
в) Конфиденциальность

6. К международным стандартам не относятся стандарты группы:

а) ISO
б) ГОСТ Р
в) IEC
г) Common Criteria for IT Security

7. Защита от несанкционированного доступа к информации – это составляющая информационной безопасности

а) Доступность
б) Целостность
в) Конфиденциальность

8. По доступности выделяют следующие виды стандартов:

а) Международные и национальные
б) Оценочные и спецификации
в) Обязательные и рекомендуемые
г) Общедоступные и распространяемые по лицензии

9. Первым и наиболее известным документом по стандартизации в области информационной безопасности является:

а) Британский стандарт BS 7799
б) Оранжевая книга (1985 г.)
в) ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

10. Потенциальная возможность определенным образом нарушить информационную безопасность – это

а) взлом
б) угроза

в) хакерская атака
г) кража информации

11. По обязательности выполнения выделяют следующие виды стандартов:

а) Международные и национальные
б) Оценочные и спецификации
в) Обязательные и рекомендуемые
г) Общедоступные и распространяемые по лицензии

12. Попытка реализации угрозы называется

а) несанкционированным доступом
б) атакой
в) уязвимостью
г) кражей

13. По территории распространения выделяют следующие виды стандартов:

а) Международные и национальные
б) Оценочные и спецификации
в) Обязательные и рекомендуемые
г) Общедоступные и распространяемые по лицензии

14. По аспекту информационной безопасности выделяют угрозы

а) доступности, целостности, конфиденциальности
б) случайные/преднамеренные, действия природного/техногенного характера
в) внутри/вне рассматриваемой ИС
г) данных, программ, аппаратуры, поддерживающей инфраструктуры

15. По расположению источника угроз выделяют угрозы

а) доступности, целостности, конфиденциальности
б) случайные/преднамеренные, действия природного/техногенного характера
в) внутри/вне рассматриваемой ИС
г) данных, программ, аппаратуры, поддерживающей инфраструктуры

16. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется:

а) угрозой
б) окном опасности
в) атакой
г) взломом

17. Из следующих утверждений выберите одно неверное

а) Пока существует окно опасности, возможны успешные атаки на ИС.
б) Потенциальные злоумышленники называются источниками угрозы.
в) Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем.
г) Пока существует окно опасности, не возможны атаки на ИС.

18. По способу осуществления выделяют угрозы доступности, целостности, конфиденциальности

а) случайные/преднамеренные, действия природного/техногенного характера
б) внутри/вне рассматриваемой ИС
в) данных, программ, аппаратуры, поддерживающей инфраструктуры

19. Отказ пользователей, внутренний отказ информационной системы, отказ поддерживающей инфраструктуры относятся к угрозам

а) доступности
б) целостности
в) конфиденциальности

20. По компонентам информационных систем, на которые угрозы нацелены, выделяют угрозы

а) доступности, целостности, конфиденциальности
б) случайные/преднамеренные, действия природного/техногенного характера
в) внутри/вне рассматриваемой ИС
г) данных, программ, аппаратуры, поддерживающей инфраструктуры

21. Ввод неверных данных, нарушение атомарности транзакций, переупорядочение, дублирование данных относятся к угрозам

а) доступности
б) целостности
в) конфиденциальности

22. К основным видам защищаемой информации, оборот которой контролируется, относятся

а) объекты промышленной собственности, объекты авторского права
б) служебная тайна, государственная тайна, объекты интеллектуальной собственности
в) профессиональная тайна, персональные данные

23. К основным видам защищаемой информации – государственных секретов, относятся

а) объекты промышленной собственности, объекты авторского права
б) служебная тайна, государственная тайна
в) профессиональная тайна, персональные данные

24. Основным содержанием внутрикорпоративной информации являются:

а) Приказы, распоряжения, расписания, отчеты собраний проектных групп, документы системы качества
б) Регистрационные и уставные документы, нормативы
в) Файлы и документы для внутреннего обмена данными
г) Фотографии, видеоролики, фильмы, аудиокниги

25. Информация, составляющая государственную тайну не может иметь гриф

а) "для служебного пользования"

б) "секретно"
в) "совершенно секретно"
г) "особой важности"

5.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

Процедура оценивания знаний, умений, навыков и (или) опыта деятельности слушателей по дисциплине «Способы обеспечения исполнения обязательств» основана на использовании технологической карты дисциплины, приведенной ниже.

Технологическая карта дисциплины

№ п/п	Показатели оценивания	Максимальное количество баллов
Промежуточная аттестация		
1	Тестирование	100
Итого промежуточная аттестация		*100*
ИТОГО по дисциплине		**100**

Максимальное количество баллов по дисциплине – 100.
Максимальное количество баллов на зачете – 100.

Шкала итоговых оценок успеваемости по дисциплине «Управление персоналом» отражена в технологической карте дисциплины:
- зачета

Количество баллов	Оценка
60 и более	зачтено
59 и менее	не зачтено

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

Основная литература:

1. Кияев, В. Безопасность информационных систем: курс / В. Кияев, О. Граничин. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. http://biblioclub.ru/index.php?page=book&id=429032
2. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н.Загинайлов. - М.-Берлин: Директ-Медиа, 2015. - 253с. http://biblioclub.ru/index.php?page=book_view&book_id=276557

Дополнительная литература:

1. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-

9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356 (05.06.2018).
2. Гаджинский, А.М. Логистика : учебник / А.М. Гаджинский. - 21-е изд. - Москва : Издательско-торговая корпорация «Дашков и К°», 2017. - 419 с. : ил. - (Серия «Учебные издания для бакалавров»). - Библиогр. в кн. - ISBN 978-5-394-02059-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=495765 (26.12.2018).
3. Каранина, Е.В. Экономическая безопасность: на уровне государства, региона, предприятия : учебник / Е.В. Каранина. - Санкт-Петербург : ИЦ "Интермедия", 2017. - 412 с. : схем., табл. - Библиогр.: с. 363-391. - ISBN 978-5-98228-099-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=482790 (26.12.2018).
4. Голов, Р.С. Организация производства, экономика и управление в промышленности : учебник / Р.С. Голов, А.П. Агарков, А.В. Мыльник. - Москва : Издательско-торговая корпорация «Дашков и К°», 2017. - 858 с. : табл., схем., граф. - (Учебные издания для бакалавров). - Библиогр. в кн. - ISBN 978-5-394-02667-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=452544 (26.12.2018).
5. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331 (05.06.2018).

Периодические издания:

1. Системный администратор
2. Беспроводные технологии
3. Мир ПК
4. Информационная безопасность

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

Информационные ресурсы образовательной организации:

1. http://www.sibit.sano.ru/ - официальный сайт образовательной организации
2. http://do.sano.ru - система дистанционного обучения Moodle (СДО Moodle)

Электронные источники и Интернет-ресурсы:

1. http://lib.perm.ru – электронная библиотека по различным отраслям информатики и информационных технологий;
2. http://www.ci.ru – электронная версия газеты «Компьютер-Информ»;
3. http://www.pcworld.ru – электронная версия журнала «Мир ПК»;
4. http://www.citforum.ru/ -электронная библиотека CITForum;
5. http://emanual.ru/ - электронная библиотека eManual.ru;
6. http://it-ebooks.ru/ - электронная библиотека системного администратора;
7. http://window.edu.ru/ - Информационная система «Единое окно доступа к образовательным ресурсам»;
8. http://biblioclub.ru - Электронная библиотечная система «Университетская библиотека онлайн»

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При осуществлении образовательного процесса слушателями и преподавателем используется следующее программное обеспечение:

Наименование	Основание	Описание	Количество лицензий
Электронные справочные системы			
Consultant Plus	Договор 11/01-09 от 01.09.2009 г. Доп.соглашение №1	ЭСС Консультант+	Неограниченно
Библиотечная система АБС ИРБИС64	Договор № 64/11-11-11 от 11.11.2011 г.	АБС	Неограниченно
ЭБС «Электронная библиотека онлайн» (biblioclub.ru)	Договор № 014-052015 от 10.06.2015 г.	ЭБС	Неограниченно
Пакеты редакторов текстовых документов, электронных таблиц			
Microsoft Office Professional Plus 2013	Open License 62668528	Пакет электронных редакторов	
Microsoft Office Professional Plus 2007	Open License 42024141	Пакет электронных редакторов	
Microsoft Office Standard 2016	Open License 66020759	Пакет электронных редакторов	
Microsoft Office Standard 2013	Open License 637269920	Пакет электронных редакторов	
Microsoft Office Standard 2007	Open License 42024141	Пакет электронных редакторов	
Microsoft Office Project 2010	Акт № ГАРТ0006235 от 25.04.2012 г.	Пакет электронных редакторов по управлению проектами	

При осуществлении образовательного процесса слушателями и преподавателем используются следующие информационно-справочные системы:

1. Электронная библиотечная система «Университетская библиотека онлайн»;
2. Интегрированная библиотечно-информационная система ИРБИС64.

Документы, подтверждающие наличие и право использования образовательной организацией электронных библиотечных систем, профессиональных баз данных и других информационных ресурсов:

1. Договор № 104-08/18 на оказание услуг по предоставлению доступа к электронным изданиям базовой коллекции ЭБС «Университетская библиотека онлайн» от 03 сентября 2018 г. (http://www.biblioclub.ru).

2. Договор № 64/19-03-18 о поставке научно-технической продукции – Системы Автоматизации Библиотек ИРБИС64 – от 19 марта 2018 г., в состав которой входит База данных электронного каталога библиотеки СИБИТ Web-ИРБИС 64 (http://lib.sano.ru)

Информационные технологии:

- занятия с использованием мультимедийных презентаций;
- проектор и экран;
- интерактивная доска;
- компьютерный класс;

- сетевая работа в виртуальном классе.

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

Для материально-технического обеспечения дисциплины «Способы обеспечения исполнения обязательств» используется:

1. Компьютерные классы, оборудованные для проведения практических занятий средствами оргтехники, персональными компьютерами, объединенными в сеть с выходом в Интернет;
2. Аудитории, оснащенные стационарным мультимедийным оборудованием (проекторы, интерактивные доски, виртуальный класс);
3. Установленное лицензионное программное обеспечение;
4. Мультимедийные презентации;
5. Подборка электронных учебно-методических материалов.

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями здоровья и инвалидов

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены вузом или могут использоваться собственные технические средства. Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на выполнение заданий текущего контроля. Процедура проведения промежуточной аттестации для обучающихся с ограниченными возможностями здоровья и обучающихся инвалидов устанавливается с учётом индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.