

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

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

Дата подписания: 01.08.2025

Уникальный программный ключ:

65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе

Дисциплины «Информационная безопасность»

Направление подготовки бакалавров «09.03.02 – Информационные системы и технологии»

Цель преподавания дисциплины

Целью преподавания дисциплины «Информационная безопасность» является изложение основ комплексной защиты информационно-коммуникационных систем на основе применения программно-аппаратных и коммуникационных технических средств, устройств и комплексов, нормативных и технических требований к системам, сетям и средствам защиты информации.

Задачи изучения дисциплины

- изучение классификации угроз информационной безопасности;
- изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- ознакомление с симметричными и ассиметричными криптосистемами, изучение алгоритмов RSA, Виженера, AES, электронно-цифровой подписи;
- изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно – программных систем идентификации и аутентификации;
- изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;
- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;
- изучение основных требований и рекомендаций по защите информации в компьютерных системах;
- изучение основных юридических законов в области защиты информации.

Компетенции, формируемые в результате освоения дисциплины

УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.

ПК-8 – Способен обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы.

ПК-11 - Способен проводить консультирование и обучение пользователей ин-формационных технологий и систем.

Разделы дисциплины

Основные понятия и анализ угроз информационной безопасности.

Проблемы информационной безопасности сетей.

Политика безопасности.

Криптографическая защита информации.

Технологии аутентификации.

Технологии межсетевых экранов.

Технологии защиты от вирусов.

Требования к системам защиты информации.

Основы правового обеспечения защиты информации.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:

И.О. декана факультета

Фундаментальной и прикладной
информатики

(наименование ф-та полностью)

 Т.А. Ширабакина
(подпись, инициалы, фамилия)«01» сентября 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

(наименование дисциплины)

ОПОП ВО 09.03.02 Информационные системы и технологии

(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Информационные технологии

наименование направленности (профиля, специализации)

в бизнесе»

форма обучения

очная

(очная, очно-заочная, заочная)

Рабочая программа дисциплины Информационная безопасность составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 09.03.02 Информационные системы и технологии на основании учебного плана ОПОП ВО 09.03.02 Информационные системы и технологии, направленность Информационные технологии в бизнесе, одобренного Ученым советом университета (протокол №7«29» 03 2019 г.).

Рабочая программа дисциплины Информационная безопасность обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 09.03.02 Информационные системы и технологии, направленность Информационные технологии в бизнесе на заседании кафедры информационной безопасности Протокол № 1 «31» 08 2020г.

Зав. кафедрой

Разработчик программы

к.в.н., доцент

Согласовано: на заседании кафедры информационных систем и технологий № 1 «31» 08 20 20 г.

Зав. кафедрой

Директор научной библиотеки

Таныгин М.О.

Ханис А.Л.

Сазонов С.Ю.

Макаровская В.Г.

Рабочая программа дисциплины Информационная безопасность пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.02 Информационные системы и технологии, направленность Информационные технологии в бизнесе, одобренного Ученым советом университета протокол №7«25» 02 2020г., на заседании кафедры ИБ, протокол №11 28.06.2021г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа дисциплины Информационная безопасность пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.02_Информационные системы и технологии, направленность «Информационные технологии в бизнесе», одобренного Ученым советом университета протокол № 9 «25» 06 2021г., на заседании кафедры информационной безопасности № 11 «30» 06 2022г.

Зав. кафедрой _____



Рабочая программа дисциплины Информационная безопасность пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.02_Информационные системы и технологии, направленность «Информационные технологии в бизнесе», одобренного Ученым советом университета протокол № 9 «25» 06 2021г., на заседании кафедры информационной безопасности № 1 «30» 08 2023г.

Зав. кафедрой _____



Рабочая программа дисциплины Информационная безопасность пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.02_Информационные системы и технологии, направленность «Информационные технологии в бизнесе», одобренного Ученым советом университета протокол № « » 20 г., на заседании кафедры информационной безопасности № « » 20 г.

Зав. кафедрой _____

Рабочая программа дисциплины Информационная безопасность пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.02_Информационные системы и технологии, направленность «Информационные технологии в бизнесе», одобренного Ученым советом университета протокол № « » 20 г., на заседании кафедры информационной безопасности № « » 20 г.

Зав. кафедрой _____

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

1.1 Цель дисциплины

Целью преподавания дисциплины «Информационная безопасность» является изложение основ комплексной защиты информационно-коммуникационных систем на основе применения программно-аппаратных и коммуникационных технических средств, устройств и комплексов, нормативных и технических требований к системам, сетям и средствам защиты информации.

1.2 Задачи дисциплины

- изучение классификации угроз информационной безопасности;
- изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- ознакомление с симметричными и асимметричными криптосистемами, изучение алгоритмов RSA, Виженера, AES, электронно-цифровой подписи;
- изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно - программных систем идентификации и аутентификации;
- изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;
- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;
- изучение основных требований и рекомендаций по защите информации в компьютерных системах;
- изучение основных юридических законов в области защиты информации.

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

Таблица 1.3 – Результаты обучения по дисциплине

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.	УК-2.1 Формулирует проблему, решение которой напрямую связано с достижением цели проекта.	Знать: виды угроз и возможные каналы утечки конфиденциальной информации, основные принципы построения политики информационной безопасности, основные виды сетевых атак и методы противодействия им. Уметь: правильно эксплуатировать антивирусные программные комплексы, снижать вероятность отрицательных последствий сетевых атак путем правильной настройки операционной системы, применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры инфо-коммуникационных систем и сетевой защиты, поиска и обнаружения уязвимых узлов инфо-коммуникационных систем и сетей.
		УК-2.2 Определяет связи между поставленными задачами и ожидаемые результаты их решения.	Знать: алгоритмы работы средств и систем защиты инфо-коммуникационных сетей, методы аутентификации и принципы работы аппаратно-

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>программных средств идентификации и аутентификации, функции, классификацию и схемы подключения межсетевых экранов.</p> <p>Уметь: правильно эксплуатировать и разрабатывать программы защиты данных, предлагать конкретные меры по усилению парольной защиты, применять антивирусные программные комплексы.</p> <p>Владеть: навыками защиты информации в компьютерных системах, навыками анализа защищенности локальной вычислительной сети, решения задач обеспечения защиты инфо-коммуникационных сетей.</p>
		<p>УК-2.3 Анализирует план-график реализации проекта в целом и выбирает оптимальный способ решения поставленных задач.</p>	<p>Знать: классификацию компьютерных вирусов, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, основные требования к системам защиты информации, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем, основные юридические законы в области защиты информации.</p> <p>Уметь: настраивать режимы работы межсетевых экранов, проводить анализ</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикатора- ми достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>защищенности локальной вычислительной сети, разрабатывать защищенные сайты с использованием языков HTML, JavaScript, PHP, проводить анализ информационных рисков.</p> <p>Владеть: навыками эксплуатации программных средств анализа и управления рисками, навыками разработки программ защиты данных, навыками разработки защищенных сайтов, разработки планов графиков разработки и установки программных средств защиты инфо-коммуникационных сетей.</p>
		<p>УК-2.4 В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы.</p>	<p>Знать: классификацию программно-аппаратных и телекоммуникационных средств, технические характеристики и возможности сетевого оборудования инфо-коммуникационных сетей, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности систем и сетей, основные действующие нормативные документы и юридические законы в области защиты информации.</p> <p>Уметь: проводить анализ защищенности локальной</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотносенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>вычислительной сети, настраивать режимы работы межсетевых экранов, проводить анализ информационных рисков, определять оптимальный состав программных и аппаратных средств для построения инфо-коммуникационных сетей, применять действующие нормативные документы и юридические законы в области защиты информации.</p> <p>Владеть: навыками выбора программно-аппаратных средств и телекоммуникационного оборудования, эксплуатации программных средств анализа и управления рисками, навыками разработки защищенных сайтов, разработки и установки программных средств защиты инфо-коммуникационных сетей, определения действующих нормативных требований и юридических законов в области защиты информации.</p>
		<p>УК-2.5 Оценивает решение поставленных задач в зоне своей ответственности в соответствии с запланированными результатами контроля, при необходимости корректирует способы решения задач.</p>	<p>Знать: методы и способы контроля бесперебойного функционирования телекоммуникационного оборудования, сетей и систем, классификацию программно-аппаратных и телекоммуникационных средств, технические характеристики и возможности сетевого оборудования инфо-коммуникационных сетей, каналы распространения</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>вредоносных программ, классификацию вирусных программ, методы обнаружения компьютерных вирусов, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности систем и сетей, методы и способы устранения неисправностей, выявленных в ходе эксплуатации инфокоммуникационных сетей.</p> <p>Уметь: применять методы и способы контроля бесперебойного функционирования инфокоммуникационных сетей, методы и способы определения неисправностей программно-аппаратного и коммутационного оборудования инфокоммуникационных сетей, проводить анализ защищенности локальной вычислительной сети, настраивать режимы работы межсетевых экранов.</p> <p>Владеть: навыками контроля бесперебойного функционирования инфокоммуникационных сетей, определения неисправностей программно-аппаратного и коммутационного оборудования инфокоммуникационных сетей, эксплуатации программных средств защиты.</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
ПК-8	Способен обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы.	ПК-8.1 Осуществляет мониторинг за работой инфокоммуникационной системы и/или ее составляющих.	<p>Знать: виды угроз и возможные каналы утечки информации, классификацию вирусных программ, классификацию и режимы функционирования телекоммуникационного оборудования, классификацию и принципы функционирования антивирусного программного обеспечения, основные виды сетевых атак и методы противодействия им.</p> <p>Уметь: эксплуатировать антивирусные программные комплексы и средства контроля функционирования телекоммуникационного оборудования, снижать вероятность отрицательных последствий сетевых атак путем правильной настройки операционной системы, применять средства защиты информации для решения практических задач в области информационной безопасности.</p> <p>Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты, средств контроля и мониторинга бесперебойного функционирования инфокоммуникационных сетей.</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикатора- ми достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
		ПК-8.2 Обнаруживает отклонения от штатного режима работы инфокоммуникационной системы и/или ее составляющих.	<p>Знать: режимы работы сетевого оборудования, требования к функционированию аппаратно-программных средств, технические характеристики телекоммуникационного оборудования, алгоритмы работы систем защиты информации, методы аутентификации и принципы работы аппаратно-программных систем идентификации и аутентификации.</p> <p>Уметь: эксплуатировать программные средства защиты и контроля функционирования режимом работы сетевого оборудования, предлагать конкретные меры по выявлению неисправностей в работе оборудования сетей и усилению парольной защиты, применять антивирусные программные комплексы.</p> <p>Владеть: навыками защиты информации в компьютерных системах, навыками анализа защищенности инфокоммуникационной сети, способами и методами диагностики функционирования оборудования в случае сетевых атак.</p>
		ПК-8.3 Анализирует отклонения от штатного режима работы инфокоммуникационной системы и/или ее составляющих.	<p>Знать: режимы работы сетевого оборудования, требования к функционированию аппаратно-программных средств, технические характеристики телекоммуникационного</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>оборудования, алгоритмы работы систем защиты информации, методы аутентификации и принципы работы аппаратно-программных систем идентификации и аутентификации.</p> <p>Уметь: анализировать режимы функционирования инфо-коммуникационных сетей, настраивать режимы работы межсетевых экранов, проводить анализ защищенности локальной вычислительной сети, разрабатывать защищенные сайты, проводить анализ информационных рисков.</p> <p>Владеть: навыками анализа уязвимых узлов инфо-коммуникационных сетей, защиты информации в компьютерных системах, навыками анализа защищенности инфо-коммуникационной сети, способами и методами диагностики функционирования оборудования в случае сетевых атак.</p>
		<p>ПК-8.4 Устраняет возникающие отклонения от штатного режима работы инфо-коммуникационной системы и/или ее составляющих.</p>	<p>Знать: ТТХ и принципы работы аппаратно-программных средств и оборудования для обеспечения информационной безопасности системы, основные этапы устранения отклонений от штатного режима работы информационной системы, методы диагностики и ремонта оборудования сетей, основные требования к</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>системам информационной безопасности; показатели защищенности средств вычислительной техники от несанкционированного доступа.</p> <p>Уметь: применять программные и технические средства анализа состояния уязвимых узлов сетей, эксплуатировать программные средства защиты и контроля функционирования режимом работы сетевого оборудования, предлагать конкретные меры по устранению неисправностей возникших в работе оборудования сетей, применять антивирусные программные комплексы.</p> <p>Владеть: навыками эксплуатации программных и аппаратных средств защиты информации, анализа и определения уязвимых узлов составных частей сетей, навыками разработки защищенных сайтов, программных средств обеспечения информационной безопасности.</p>
ПК-11	Способен проводить консультирование и обучение пользователей информационных технологий и систем.	ПК-11.1 Осуществляет разработку и выбор программ обучения пользователей информационных технологий и систем.	<p>Знать: виды угроз и возможные каналы утечки информации в ИС, классификацию вирусных программ, классификацию и режимы функционирования телекоммуникационного оборудования ИС, классификацию и принципы функционирования антивирусного программного обеспечения, основные виды сетевых атак и методы противодействия им.</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикатора- ми достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>Уметь: эксплуатировать антивирусные программные комплексы и средства, снижать вероятность отрицательных последствий сетевых атак путем правильной настройки компонентов ИС, применять средства защиты информации для решения практических задач в области безопасности функционирования ИС.</p> <p>Владеть: навыками разработки программ обучения на основе применения программных средств защиты информации в ИС, разработки защищенных сайтов, диагностики ИС с целью их бесперебойного функционирования, разработки программных приложений на базе языков.</p>
		<p>ПК-11.2 Проводит обучение пользователей информационных технологий и систем по сложным программам обучения</p>	<p>Знать: виды угроз и возможные каналы утечки информации в ИС, классификацию вирусных программ, классификацию и режимы функционирования телекоммуникационного оборудования ИС, классификацию и принципы функционирования антивирусного программного обеспечения, основные виды сетевых атак и методы противодействия им.</p> <p>Уметь: эксплуатировать антивирусные программные комплексы и средства, снижать вероятность отрицательных последствий сетевых атак путем</p>

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной	Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций
код компетенции	наименование компетенции		
			<p>правильной настройки компонентов ИС, применять средства защиты информации для решения практических задач в области безопасности функционирования ИС.</p> <p>Владеть: навыками разработки программ обучения на основе применения программных средств защиты информации в ИС, разработки защищенных сайтов, диагностики ИС с целью их бесперебойного функционирования.</p>
		<p>ПК-11.3 Осуществляет выходное тестирование пользователей информационных технологий и систем.</p>	<p>Знать: виды угроз и возможные каналы утечки информации в ИС, классификацию вирусных программ, классификацию и режимы функционирования телекоммуникационного оборудования ИС, классификацию и принципы функционирования антивирусного программного обеспечения, основные виды сетевых атак и методы противодействия им.</p> <p>Уметь: эксплуатировать антивирусные программные комплексы и средства, снижать вероятность отрицательных последствий сетевых атак путем правильной настройки компонентов ИС, применять средства защиты информации для решения практических задач в области безопасности функционирования ИС.</p> <p>Владеть: навыками разработки программ</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикатора- ми достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>обучения на основе применения программных средств защиты информации в ИС, разработки защищенных сайтов, диагностики ИС с целью их бесперебойного функционирования, разработки программных приложений на базе языков.</p>
		<p>ПК-11.4 Анализирует замечания и пожелания пользователей для развития ИС.</p>	<p>Знать: виды угроз и возможные каналы утечки информации в ИС, классификацию вирусных программ, классификацию и режимы функционирования телекоммуникационного оборудования ИС, классификацию и принципы функционирования антивирусного программного обеспечения, основные виды сетевых атак и методы противодействия им.</p> <p>Уметь: эксплуатировать антивирусные программные комплексы и средства, снижать вероятность отрицательных последствий сетевых атак путем правильной настройки компонентов ИС, применять средства защиты информации для решения практических задач в области безопасности функционирования ИС.</p> <p>Владеть: навыками разработки программ обучения на основе применения программных средств защиты информации в ИС, разработки защищенных сайтов, диагностики ИС с целью их бесперебойного</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			функционирования.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Элективная дисциплина «Информационная безопасность», входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы бакалавриата (специалитета, магистратуры) 09.03.02 Информационные системы и технологии, направленность Информационные технологии в бизнесе. Дисциплина изучается на 4 курсе в 7 семестре.

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

Общая трудоемкость (объем) дисциплины составляет 3 зачетные единицы (з.е.), 108 академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	54
в том числе:	
лекции	18
лабораторные занятия	18
практические занятия	18
Самостоятельная работа обучающихся (всего)	53,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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

4.1 Содержание дисциплины

Таблица 4.1.1 - Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел, (тема) дисциплины	Содержание
1	2	3
1	Основные понятия и анализ угроз информационной безопасности	Основные понятия защиты информации и информационной безопасности. Понятие угрозы информационной безопасности. Анализ и классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности информации, целостности информации, доступности информации. Угроза раскрытия параметров автоматизированной системы.
2	Проблемы информационной безопасности сетей	Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP- сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности компьютерных сетей. Пути решения проблем защиты информации в сетях.
3	Политика безопасности	Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Основные этапы разработки политики безопасности организации. Компоненты архитектуры безопасности сети:

4	Криптографическая защита информации	Основные понятия криптографической защиты информации. Требования к криптографическим системам. Симметричные и асимметричные крипто-системы шифрования. Блочные и потоковые шифры. Шифры простой замены. Шифры Виженера. Стандарт шифрования AES. Алгоритм шифрования RSA. Функция хэширования. Электронная цифровая подпись (ЭЦП). Защита электронного документооборота с использованием ЭЦП. Обзор программных и программно-аппаратных средств криптографической защиты.
5	Технологии аутентификации	Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоцветных паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутентификация пользователя. Аппаратно-программные системы идентификации и аутентификации.
6	Технологии межсетевых экранов	Классификация межсетевых экранов. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий. Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.
7	Технологии защиты от вирусов	Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод "белого списка", обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ. Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети.

8	Требования к системам защиты информации	Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.
9	Основы правового обеспечения защиты информации	Правовое обеспечение информационной собственности и его место в системе информационного права. Информация как объект юридической защиты. Формирование государственной системы правового обеспечения информационной безопасности. Правовое обеспечение защиты государственной тайны. Законодательство Российской Федерации в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Правовая защита интеллектуальной собственности. Правовое регулирование деятельности организаций в области информационной безопасности.

Таблица 4.1.2 - Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра)	Компетенции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Основные понятия и анализ угроз информационной безопасности	2	-	-	У-1, У-2, У-3, У-4, У-5, У-7, МУ-7	УО - 2	УК-2
2	Проблемы информационной безопасности сетей	2	-	-	У-2, У-7, У-10, МУ-7	УО - 4	УК-2, ПК-8
3	Политика безопасности	2	1	-	У-1, У-3, У-5, У-7, МУ-1, МУ-7	УО, ЗЛР - 6	ПК-8, ПК-11
4	Криптографическая защита информации	2	-	1,2	У-1, У-4, У-7,	УО – 8 ЗЛР – 4,8	ПК-8, ПК-11

					МУ-5-7		
5	Технологии аутентификации	2	-	3	У-4, У-6, У-7, У-10, МУ-5-7	УО, ЗЛР - 10	ПК-8, ПК-11
6	Технологии межсетевых экранов	2	-	-	У-1, У-2, У-4, У-6, У-9, У-10, МУ-7	УО - 12	ПК-8, ПК-11
7	Технологии защиты от вирусов	2	-	-	У-2, У-4, У-8, У-9, У-10, МУ-7	УО - 14	ПК-8, ПК-11
8	Требования к системам защиты информации	2	2,3,4	-	У-1-6, У-10, МУ-2-4, МУ-7	УО – 16 ЗЛР – 12,14,16	ПК-8, ПК-11
9	Основы правового обеспечения защиты информации	2	-	-	У-1-7, МУ-7	УО - 18	ПК-8, ПК-11
	Всего	18	18	18			

УО – устный опрос, ЗЛР – лабораторная работа, ЗЛР – практическая работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 - Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	Анализ и управление информационными рисками в программе “Триф”	4
2	Создание сайтов на языке JavaScript и обеспечение их информационной безопасности	4
3	Создание сайтов на языках HTML и обеспечение их информационной безопасности	4
4	Разработка и защита Web-приложений с серверными сценариями на языке PHP	6
Итого		18

4.2.2 Практические занятия

Таблица 4.2.2 - Практические занятия

№	Наименование практического (семинарского) занятия	Объем, час.
---	---	-------------

1	Настройка межсетевого экрана Comodo Firewall.	6
2	Антивирусная программа: Kaspersky Internet Security	6
3	Анализ защищенности компьютерной сети с помощью программ GFI LANguard Network Security Scanner и	6
Итого		18

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Основные понятия и анализ угроз информационной безопасности	2 неделя	4,9
2	Проблемы информационной безопасности сетей	4 неделя	5
3	Политика безопасности	6 неделя	6
4	Криптографическая защита информации	8 неделя	6
5	Технологии аутентификации	10 неделя	6
6	Технологии межсетевых экранов	12 неделя	6
7	Технологии защиты от вирусов	14 неделя	6
8	Требования к системам защиты информации	16 неделя	7
9	Основы правового обеспечения защиты информации	18 неделя	7
Итого			53,9

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

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

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

библиотекой университета:

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

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

кафедрой:

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

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

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачёту;

– методических указаний к выполнению лабораторных и практических работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

– удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

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

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
1	Лекция №1. Основные понятия и анализ угроз информационной безопасности.	Анализ конкретных ситуаций	1
2	Лекция №2. Проблемы информационной безопасности сетей.	Анализ конкретных ситуаций	1
3	Лекция №3. Политика безопасности.	Анализ конкретных ситуаций	1
4	Лекция №8. Требования к системам защиты информации.	Анализ конкретных ситуаций	1
5	Практическое занятие №1	Анализ конкретных ситуаций	2
6	Практическое занятие №2.	Анализ конкретных ситуаций	2

7	Практическое занятие №3	Анализ конкретных ситуаций	4
Итого			12

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения лабораторных занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю, специализации) программы бакалавриата.

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

- целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для природы, человека и общества;

- применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, представителями работодателей (командная работа, разбор конкретных ситуаций, и др.);

- личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности,

ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

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

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

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющих ресурсы и ограничений.	Экономика. Правоведение. Введение в направление подготовки и планирование профессиональной карьеры.	Социология. Экология. Проектный практикум.	Защита информации. Выполнение и защита выпускной квалификационной работы.
ПК-8. Способен обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы.	Архитектура вычислительных систем и компьютерных сетей.	Эконометрика. Предметно-ориентированные экономические информационные системы. Учебная эксплуатационная практика. Производственная технологическая (проектно-технологическая) практика.	Защита информации. Операционные системы. Цифровая обработка и анализ изображений. Информационные системы и технологии в бизнесе. Выполнение и защита выпускной квалификационной работы.

<p>ПК-11. Способен проводить консультирование и обучение пользователей информационных технологий и систем.</p>		<p>Электронный бизнес. Инновационный менеджмент. Управление инновациями. Производственная преддипломная практика.</p>	<p>Защита информации. Информационные системы бухгалтерского учета. Выполнение и защита выпускной квалификационной работы.</p>
--	--	---	---

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

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисциплиной)	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
<p>УК-2, завершающий.</p>	<p>УК-2.1 Формулирует проблему, решение которой напрямую связано с достижением цели проекта.</p>	<p>Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.</p>	<p>Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных</p>	<p>Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ</p>

	<p>УК-2.2 Определяет связи между поставленными задачами и ожидаемые результаты их решения.</p>	<p>Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.</p>	<p>средств защиты информации, разработки защищенных сайтов. Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.</p>	<p>информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты. Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.</p>
	<p>УК-2.3 Анализирует план-график реализации проекта в целом и выбирает оп-</p>	<p>Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических за-</p>	<p>Знать: методы защиты информации, способы защиты сайтов. Уметь: применять</p>	<p>Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информа-</p>

	<p>тимальный способ решения поставленных задач.</p>	<p>дач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.</p>	<p>средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.</p>	<p>ционной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.</p>
	<p>УК-2.4 В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы.</p>	<p>Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.</p>	<p>Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.</p>	<p>Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программ-</p>

				ных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	<p>УК-2.5</p> <p>Оценивает решение поставленных задач в зоне своей ответственности в соответствии с запланированными результатами контроля, при необходимости корректирует способы решения задач.</p>	<p>Знать: методы защиты информации.</p> <p>Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности.</p> <p>Владеть: навыками применения программных средств защиты информации.</p>	<p>Знать: методы защиты информации, способы защиты сайтов.</p> <p>Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты.</p> <p>Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.</p>	<p>Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности.</p> <p>Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков.</p> <p>Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.</p>
ПК-8, завершающий.	ПК-8.1 Осуществляет мониторинг за работой информационной системы и/или ее составляющих.	<p>Знать: методы защиты информации.</p> <p>Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности.</p> <p>Владеть: навыками приме-</p>	<p>Знать: методы защиты информации, способы защиты сайтов.</p> <p>Уметь: применять средства защиты информации для решения практических задач в области инфор-</p>	<p>Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности.</p> <p>Уметь: применять средства защиты информации для решения прак-</p>

	<p>ПК-8.2 Обнаруживает отклонения от штатного режима работы информационно-коммуникационной системы и/или ее составляющих.</p>	<p>Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.</p>	<p>мационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов. Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.</p>	<p>тических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты. Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты. Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков ин-</p>
	<p>ПК-8.3 Анализирует отклонения от штатного режима работы инфо-</p>	<p>Знать: методы защиты информации. Уметь: применять средства защиты информации</p>	<p>Знать: методы защиты информации, способы защиты сайтов. Уметь:</p>	

	<p>коммуникационной системы и/или ее составляющих.</p> <p>ПК-8.4 Устраняет возникающие отклонения от штатного режима работы инфокоммуникационной системы и/или ее составляющих.</p>	<p>для решения практических задач в области информационной безопасности.</p> <p>Владеть: навыками применения программных средств защиты информации.</p> <p>Знать: методы защиты информации.</p> <p>Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности.</p> <p>Владеть: навыками применения программных средств защиты информации.</p>	<p>применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты.</p> <p>Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.</p> <p>Знать: методы защиты информации, способы защиты сайтов.</p> <p>Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты.</p> <p>Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.</p>	<p>формационной безопасности.</p> <p>Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков.</p> <p>Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.</p> <p>Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности.</p> <p>Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков.</p> <p>Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.</p>
--	---	---	---	--

ПК-11, завершаю- щий.	ПК-11.1 Осуществляет разработку и выбор программ обучения пользователей информационных технологий и систем.	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ПК-11.2 Проводит обучение пользователей информационных технологий и систем по сложным программам обучения.	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков.

	<p>ПК-11.3 Осуществляет выходное тестирование пользователей информационных технологий и систем.</p>	<p>Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.</p>	<p>средств защиты информации, разработки защищенных сайтов. Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.</p>	<p>Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты. Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты. Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информаци-</p>
	<p>ПК-11.4 Анализирует замечания и пожелания пользователей для развития ИС.</p>	<p>Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты ин-</p>	<p>Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разра-</p>	<p>Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информаци-</p>

		формации.	батывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	онной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
--	--	-----------	--	--

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

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные понятия и анализ угроз информационной безопасности	УК-2	Лекция, СРС	Вопросы для устного опроса	1-3	Согласно таблице 7.2
2	Проблемы информационной безопасности сетей	УК-2, ПК-8	Лекция, СРС	Вопросы для устного опроса	4-14	Согласно таблице 7.2
3	Политика безопасности	ПК-8, ПК-11	Лекция, СРС, лабораторная работа №1	Вопросы для устного опроса <u>КВЗЛР №1</u>	15-17 1-4	Согласно таблице 7.2
4	Криптографическая защита информации	ПК-8, ПК-11	Лекция, практические работы №1 №2, СРС	Вопросы для устного опроса КВЗЛР №1 КВЗЛР №2	18-24 1 – 3 1 – 3	Согласно таблице 7.2
5	Технологии аутентификации	ПК-8, ПК-11	Лекция, практическая работа №3, СРС	Вопросы для устного опроса КВЗЛР №3	25-30 1 - 4	Согласно таблице 7.2
6	Технологии межсетевых экранов	ПК-8, ПК-11	Лекция, СРС	Вопросы для устного опроса	31-33	Согласно таблице 7.2
7	Технологии	ПК-8, ПК-11	Лекция, СРС	Вопросы для устного опроса	34-41	Согласно таблице 7.2

	защиты от вирусов					
8	Требования к системам защиты информации	ПК-8, ПК-11	Лекция, лабораторные работы №2,3,4, СРС	Вопросы для устного опроса КВЗЛР №2 КВЗЛР №3 КВЗЛР №4	42-46 1-4 1-4 1-4	Согласно таблице 7.2
9	Основы правового обеспечения защиты информации	ПК-8, ПК-11	Лекция, СРС	Вопросы для устного опроса	47-60	Согласно таблице 7.2

СРС – самостоятельная работа студента, КВЗЛР – контрольные вопросы для защиты лабораторных работ, КВЗЛР - контрольные вопросы для защиты практических работ

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 1. «Основные понятия и анализ угроз информационной безопасности».

1. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: угадывание ключа, атаки на уровне приложений, сетевая разведка, злоупотребление доверием.
2. Основные характеристики спама и методы борьбы с ним.
3. Виды интернет - мошенничества: фишинг и фарминг и методы борьбы с ними.
4. Угрозы и уязвимости проводных корпоративных сетей.

Контрольные вопросы для защиты практической работы №3:

Анализ защищенности компьютерной сети с помощью программ GFI LANguard Network Security Scanner и XSpider

1. Основные компоненты модели адаптивной безопасности
2. Принцип работы средств анализа защищенности сетевых протоколов
3. Современные средства анализа защищенности
4. Методы анализа сетевой информации, используемые в средствах обнаружения сетевых атак

Контрольные вопросы для защиты лабораторной работы №2

Разработка Web - приложений на языке HTML

1. Структура HTML документа
2. Уровни заголовков в спецификации HTML
3. Разметка абзацев в HTML
4. Вывод текста шрифтом Arial.

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачёта.

Промежуточная аттестация по дисциплине проводится в форме зачёта. Зачёт проводится в виде бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Виды информационной безопасности:

- a. Персональная, корпоративная, государственная
- b. Клиентская, серверная, сетевая
- c. Локальная, глобальная, смешанная

Задание в открытой форме:

1. ... – это сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации. Назовите субъекты информационных отношений.

2. ... информации заключается в ее существовании в неискаженном виде, не измененном по отношению к некоторому ее исходному состоянию.

3. ... свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.

4. ... свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей.

Задание на установление правильной последовательности.

Выберите правильную последовательность этапов разработки профиля защиты.

1. Анализ среды применения ИТ-продукта с точки зрения
2. безопасности.
3. Выбор профиля-прототипа.
4. Синтез требований.

Задание на установление соответствия:

1) Принцип разумной достаточности	a) защита не должна обеспечиваться только за счет секретности структурной безопасности и алгоритмов функционирования ее подсистемы.
2) Принцип разумной избыточности	b) Должны быть реализованы принципы гибкости управления, обеспечивающие возможность настройки механизмов в процессе функционирования системы.
3) Принцип гибкости управления и применения	c) на этапе разработки системы защиты в нее должна закладываться некий потенциал, который позволил бы увеличить срок ее жизнеспособности.
4) Открытость алгоритмов и механизмов защиты	d) Необходимо правильно выбрать тот уровень защиты, при котором затраты, риск взлома и размер возможного ущерба были бы приемлемыми.

Компетентностно-ориентированная задача:

Определите информационный объём сообщения в байтах, если в греческом алфавите 24 буквы и сообщение на греческом языке, содержащее 150 символов, было записано в коде Unicode. Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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

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

– положение П 02.016–2018 О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

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

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

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Устный опрос по теме 1	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 2	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 3	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 4	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 5	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 6	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме	1	Доля правильных	2	Доля правильных от-

7		ответов от 50% до 90%		ветов более 90%
Устный опрос по теме 8	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 9	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Практическая работа № 1	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа № 2	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа № 3	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Лабораторная работа №1	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Лабораторная работа №2	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Лабораторная работа №3	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Лабораторная работа №4	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование – 36 баллов.

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

8.1 Основная учебная литература

1. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 «Информационная безопасность», 400301 «Юриспруденция», 380301 «Экономика»] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. : ил., табл. - Библиогр.: с. 188-195. - ISBN 978-5-7681-1196-0 : 290.00 р. - Текст : непосредственный.

2. Информационные системы в экономике : учебное пособие для студентов вузов, обучающихся по направлению подготовки 38.03.01 "Экономика" (квалификация (степень) "бакалавр") / под ред. Д. В. Чистова. - Москва : Инфра-М, 2019. - 234 с. - (Высшее образование. Бакалавриат). - ISBN 978-5-16-003511-6 : 605.86 р. - Текст : непосредственный.

3. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. - Режим доступа : <http://biblioclub.ru/index.php?page=book&id=276557>

8.2 Дополнительная учебная литература

4. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

5. Заика, А. Компьютерная безопасность [Электронный ресурс] / А. Заика. - М. : РИПОЛ классик, 2013. - 160 с. - Режим доступа : <http://biblioclub.ru/index.php?page=book&id=227317>

6. Безбогов, А. А. Методы и средства защиты компьютерной информации [Электронный ресурс] : учебное пособие / А. А. Безбогов, А. Я. Яковлев, В. Н. Шамкин. - Тамбов : ТГТУ, 2006. - 196 с. - Режим доступа: <http://window.edu.ru/resource/546/38546>

7. Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Текст : непосредственный. Ч. 1. - 150 с. : ил., табл.

8. Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Текст : непосредственный. Ч. 2. - 303 с. : ил., табл.

8.3 Перечень методических указаний

1. Анализ и управление информационными рисками в программе “Гриф” : методические указания по выполнению лабораторных работ для

студентов направления подготовки (специальности) 09.03.02 Информационные системы и технологии / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. - Электрон. текстовые дан. (541 КБ). - Курск : ЮЗГУ, 2021. - 36 с. : ил., табл. - Загл. с титул. экрана. - Б. ц.

2. Создание сайтов на языке JavaScript и обеспечение их информационной безопасности : методические указания по выполнению лабораторных работ для студентов направления подготовки (специальности) 09.03.02 Информационные системы и технологии / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. - Электрон. текстовые дан. (584 КБ). - Курск : ЮЗГУ, 2021. - 41 с. : ил., табл. - Загл. с титул. экрана. - Б. ц. - Текст : электронный.

3. Создание сайтов на языках HTML и обеспечение их информационной безопасности : методические указания по выполнению лабораторных работ для студентов направления подготовки (специальности) 09.03.02 Информационные системы и технологии / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. - Электрон. текстовые дан. (439 КБ). - Курск : ЮЗГУ, 2021. - 26 с. - Загл. с титул. экрана. - Б. ц. - Текст : электронный.

4. Разработка и защита Web-приложений с серверными сценариями на языке PHP : методические указания по выполнению лабораторных работ для студентов направления подготовки (специальности) 09.03.02 Информационные системы и технологии / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. - Электрон. текстовые дан. (376 КБ). - Курск : ЮЗГУ, 2021. - 32 с. : ил., табл. - Загл. с титул. экрана. - Б. ц.

5. Фаервол Comodo Firewall [Электронный ресурс] : методические указания по выполнению лабораторных и практических занятий по дисциплинам «Защита информационных процессов в компьютерных системах» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00, 09.00.00, 38.00.00 / Юго-Зап. гос. ун-т ; сост. К. А. Тезик. - Курск : ЮЗГУ, 2018. - 15 с. - Текст : электронный.

6. Анализ защищенности компьютерной сети с помощью программ GFI LANguard Network Security Scanner и XSpider : методические указания по выполнению практических работ для студентов направления подготовки (специальности) 09.03.02 Информационные системы и технологии / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. - Электрон. текстовые дан. (774 КБ). - Курск : ЮЗГУ, 2021. - 12 с. - Загл. с титул. экрана. - Б. ц.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца

2. Журнал «Information Security/Информационная безопасность.»- <http://window.edu.ru/>

3. Журнал «Проблемы информационной безопасности. Компьютерные системы»- <http://window.edu.ru/>

4. Журнал «Вестник УрФО. Безопасность в информационной сфере»

5. Журнал «Вопросы защиты информации»

6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»

7. Журнал «Информация и безопасность.»

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

1. <http://e.lanbook.com> - Электронно-библиотечная система «Лань».

2. <http://www.iqlib.ru> - Электронно-библиотечная система IQLib.

3. <http://window.edu.ru> -Электронная библиотека «Единое окно доступа к образовательным ресурсам».

4. <http://biblioclub.ru> – Электронно-библиотечная система «Университетская библиотека онлайн».

5. <http://www.fsb.ru> - Федеральная служба безопасности [официальный сайт].

6. <http://fstec.ru> - Федеральная служба по техническому и экспортному контролю [официальный сайт].

7. <http://microsoft.com> - Корпорация Microsoft[официальный сайт].

8. <http://www.consultant.ru> Компания«Консультант Плюс» [официальный сайт].

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность» являются лекции, практические и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

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

Изучение наиболее важных тем или разделов дисциплины завершают практические и лабораторные занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение

опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

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

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Защита информационных процессов в компьютерных системах»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

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

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

Основная цель самостоятельной работы студента при изучении дисциплины «Информационная безопасность» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

Программа анализа и управления информационными рисками “Гриф”.(свободное ПО).

Программа хранения паролей Password Commander(свободное ПО).

Фаервол Comodo Firewall (свободное ПО).

Программа анализа защищенности операционной системы GFILAN-guard Network Security Scanner.

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

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

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

Криптографическая программа TrueCrypt.

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

Учебная аудитория для проведения занятий лекционного типа и лабораторий кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проекторinFocusIN24+

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практиче-

ские задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочесть задание, оформить ответ, общаться с преподавателем).

14. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Изменённых	Заменённых	Аннулированных	новых			