

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УНИВЕРСИТЕТ УПРАВЛЕНИЯ «ТИСБИ»**

Кафедра информационных технологий



Рабочая программа дисциплины

Наименование дисциплины	Безопасность систем и сетей хранения, обработки и передачи информации
Направление подготовки	09.03.01 Информатика и вычислительная техника
Направленность (профиль) образовательной программы	Инженерия информационных систем
Год набора	2025, 2026

Составители:

Декан факультета компьютерных и инженерных наук, профессор лаборатории программной инженерии Маццара М.

Старший преподаватель лаборатории языков программирования и компиляторов Потёмкин А.С.

АНО ВО «Университет Иннополис»

Казань

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Разделы рабочей программы:

1. Краткая характеристика дисциплины (модуля).
2. Перечень планируемых результатов обучения.
3. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы высшего образования (ОПОП ВО).
4. Объем, структура и содержание дисциплины (модуля).
5. Учебно-методическое обеспечение.
6. Материально-техническое обеспечение.
7. Оценочные и методические материалы.
8. Дополнительные сведения.

Программа составлена в соответствии с требованиями ОПОП ВО Университета Иннополис по данному направлению подготовки.

Форма обучения	Семестр	Трудоемкость дисциплины в		Контактная работа		Контроль, час.	Самостоятельная работа, час.	Форма промежуточной аттестации (экз./диф.зач./зач.)
		зачетных единиц	академических часах	Лекции, час.	Семинарские (практические) занятия, час.			
очная	7	5	180	30	30	18	102	экзамен

1. КРАТКАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ (МОДУЛЯ)

Изучение дисциплины (модуля) «Security / Безопасность систем и сетей хранения, обработки и передачи информации» обеспечивает формирование и развитие компетенций обучающихся в области безопасности информации и конфиденциальности с использованием криптографических методов, их применение для решения различных прикладных задач в рамках профессиональной деятельности. В ходе освоения дисциплины обучающиеся изучают различные теоретические аспекты защиты информации и применяют на практике современные алгоритмы по защите информации.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Целью освоения дисциплины (модуля) является формирование знаний, умений и навыков в рамках профессиональной деятельности, позволяющих успешно работать в избранной отрасли, а также обладать компетенциями, способствующими социальной мобильности, устойчивости и конкурентоспособности обучающегося в условиях современных рыночных отношений. Задачами дисциплины являются изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

№ п/п	Код компетенции	Наименование компетенции	Показатели достижения результата	Формы и методы обучения, способствующие формированию и развитию компетенции
1.	ПК-1	Способен разрабатывать требования и проектировать программное обеспечение, создавать и поддерживать среды разработки, автоматизировать и контролировать качество разработки программных решений для информационных систем	Знать: основы структурного, объектно-ориентированного и функционального программирования; стандартные и прикладные библиотеки для выбранного языка программирования; принципы включения стороннего исходного кода (в том числе открытого) в разрабатываемые решения жизненный цикл и этапы разработки ПО; компилируемые и скриптовые языки программирования; языки разметки и представления/хранения данных; архитектуру баз данных (SQL / NoSQL); языки запросов к базам данных (SQL); паттерны проектирования про-	Метод анализа конкретных ситуаций, ситуационные задачи и упражнения; Метод дискуссии; Метод контрольных вопросов; Проектная технология; Информационно – коммуникационная технология

			граммного кода; архитектуры приложений; общие принципы работы операционных систем; принципы работы микросервисной архитектуры; принципы взаимодействия с API удаленных сервисов (REST, SOAP, PRC); системы управления проектами и задачами (Jira, YouTrack и др.); методики управления IT-проектами; инструменты и методы прототипирования пользовательского интерфейса. Уметь: писать поддерживаемый код на различных языках программирования; определять архитектуру приложений ИС, их масштабируемость; устанавливать и настраивать серверы баз данных; работать с инструментами и методами обработки BigData; эффективно использовать инструменты и системы контроля версий; работать с контейнерами и виртуальными машинами; управлять изменениями в приложениях и автоматизировать их; оценивать временные и материальные затраты на разработку отдельных компонент информационных систем. Владеть: методами и приемами формализации задач, методами и средствами проектирования программного обеспечения, проектирования программных интерфейсов, проектирования баз данных; навыками автоматизированной проверки и заливки кода, сборки компонентов программного решения.	
2.	ПК-2	Способен выполнять работы по созданию (модификации) и сопровождению информационных систем	Знать: архитектуру, устройство и функционирование вычислительных и информационных систем; устройство и функционирование современных информационных систем; современные стандарты информационного взаимодействия систем; программные средства и платформы инфраструктуры информационных технологий организаций; современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP, ITIL, ITSM); методы выявления требований. Уметь: разрабатывать архитектуру	Метод анализа конкретных ситуаций, ситуационные задачи и упражнения; Метод дискуссии; Метод контрольных вопросов; Проектная технология; Информационно – коммуникационная технология

			ру, дизайн и прототипы информационной системы; разрабатывать метрики (количественные показатели) работы информационной системы; настраивать и создавать компоненты анализа программного решения информационной системы; исправлять дефекты и несоответствия в архитектуре и дизайне информационной системы, подтверждать исправление дефектов и несоответствий в коде информационной системы и документации к ней; проверять (верифицировать) архитектуру информационной системы, выполнять параметрическую настройку информационной системы; разрабатывать технологии обмена данными; разрабатывать базы данных информационной системы; осуществлять оптимизацию информационной системы; разрабатывать пользовательскую документацию; оценивать временные и материальные затраты на разработку информационной системы при заданных ресурсах. Владеть: методами оптимизации работы информационной системы и её компонентов; приемами интеграции информационной системы с техническим обеспечением заказчика.	
3.	ПК-4	Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения информационных си-	Знать: общие принципы функционирования аппаратных, программных и программно-аппаратных средств информационной сети; архитектуру аппаратных, программных и программно-аппаратных средств информационной сети; средства защиты от несанкционированного доступа операционных систем и систем управления базами данных; инструкции по установке и эксплуатации администрируемых сетевых устройств и программного обеспечения; протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем, модель ISO для управления сетевым трафиком, модели IEEE, защищенные протоколы управления, основные средства криптографии;	Метод анализа конкретных ситуаций, ситуационные задачи и упражнения; Метод дискуссии; Метод контрольных вопросов; Проектная технология;

		стем	регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе; требования охраны труда при работе с сетевой аппаратурой информационной сети; особенности реализации полностью облачных и гибридных решений; инструменты CI/CD. Уметь: выяснять приемлемые для пользователей параметры работы сети в условиях нормальной (обычной) работы (базовые параметры); применять аппаратные, программные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа; пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; осуществлять мониторинг сетевых устройств; использовать современные стандарты параметризации программного обеспечения сетевой инфокоммуникационной системы; использовать типовые процедуры восстановления данных, определять точки восстановления данных, работать с серверами архивирования и средствами управления операционных систем; составлять график модернизации программно-аппаратных средств, работать с информацией организаций-производителей сетевых устройств и программного обеспечения; отслеживать развитие инфокоммуникационных технологий; обосновывать предложения по реализации стратегии в области инфокоммуникационных технологий; создавать и поддерживать инфраструктуру для разработки с применением российских программных решений и решений с открытым исходным кодом; выбирать систему оркестрации контейнеров; применять практики непрерывной интеграции, тестирования и сборки; настраивать системы непрерывной интеграции с использованием российских программных решений и решений с открытым исходным кодом; решать задачи по деплою под разные языки программирования и платформы; выбирать и настраивать необходимые серви-	Информационно – коммуникационная технология
--	--	-------------	--	--

			сы для мониторинга как отдельных приложений так и информационной системы в целом; оценивать временные и материальные затраты на развертывание программно-аппаратных решений. Владеть: навыками установки, настройки и управления локальными и глобальными сетями; настройки и управления конфигурацией нескольких серверов; современными средствами контроля производительности сети; навыками настройки параметров современных программно-аппаратных межсетевых экранов, сегментирования элементов сети; автоматизированного развертывания программного решения на стороне пользователя; навыками развертывания информационной системы, в том числе рабочих мест информационной системы у заказчика; разработки технологий интеграции информационной системы с существующими информационными системами организации; установки и настройки прикладного программного обеспечения, необходимого для функционирования информационной системы; настройки оборудования, участвующего в работе информационной системы.	
--	--	--	---	--

Знания: сформированы систематические знания средств и методов предотвращения и обнаружения вторжений; технических каналов утечки информации; технических средств перехвата информации; способов и средств защиты информации от утечки по техническим каналам; способов и средств контроля эффективности защиты информации; организации защиты информации от утечки по техническим каналам на объектах информатизации; методологии определения целей и задач принятия решений и проведения экспериментальных исследований; лексики, представляющей нейтральный научный стиль, а также основной терминологии своей специальности; продуктивного применения в типичных ситуациях основ профессиональной этики; методов и способов самоорганизации и самообразования.

Умения: сформированы умения пользоваться нормативными документами по противодействию технической разведке; применять изученные средства и методы предотвращения вторжений на практике; использовать средства защиты информации от утечки по техническим каналам; использовать средства контроля эффективности защиты информации; оценивать качество готового программного обеспечения; проводить экспериментальные исследования, применять методы планирования экспериментов, анализировать результаты экспериментальных ис-

следований; извлекать информацию по современным проблемам, правильно строить устную и письменную речь; работать в команде; корректно выражать и аргументированно обосновывать положения предметной области знания, интерпретировать полученные в практической деятельности результаты.

Навыки (владения): сформировано владение навыками технической защиты информации; владение методами расчета показателей технической защиты информации; методами инструментального контроля показателей технической защиты информации; владение современными инструментальными средствами поддержки принятия решений и планирования экспериментов и анализа их результатов; стандартными средствами базовых информационных процессов и технологий; владение навыками межличностного и группового взаимодействия в общении; навыками бесконфликтной работы и толерантного поведения при работе в коллективе.

3. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВЫСШЕГО ОБРАЗОВАНИЯ (ОПОП ВО)

Данная учебная дисциплина (модуль) включена в «Блок 1. Дисциплины (модули)» образовательной программы по направлению подготовки 09.03.01 Информатика и вычислительная техника, направленность (профиль) образовательной программы «Инженерия информационных систем» и относится к части, формируемой участниками образовательных отношений, обеспечивает формирование профессиональных компетенций. Дисциплина (модуль) «Security / Безопасность систем и сетей хранения, обработки и передачи информации» позволяет обучающимся получить знания, умения и навыки для успешной профессиональной деятельности в области программного обеспечения компьютерных вычислительных систем и сетей, автоматизированных систем обработки информации и управления. Дисциплина осваивается студентами при обучении в очной форме на 3 курсе в 7 семестре.

4. ОБЪЕМ, СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) составляет:

5 зачетных единиц, 180 академических часов, объем контактной работы — 60 академических часов.

Структура дисциплины (модуля):

№ раздела	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы			
		Очная форма			
		Контактная работа		Контроль, час.	Самостоятельная работа, час.
		Лекции, час.	Семинарские (практические) занятия, час.		
1.	Основополагающие положения	10	10	0	34

2.	Основные положения теории информационной безопасности	10	10	0	34
3.	Защита информации	10	10	0	34
	Промежуточная аттестация - экзамен			18	
ИТОГО:		30	30	18	102

Содержание дисциплины (модуля):

№ раз-дела	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам	Формируемые компетенции
1.	Основополагающие положения	Международные стандарты информационного обмена. Виды противников или «нарушителей». Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	ПК-1; ПК-2; ПК-4
2.	Основные положения теории информационной безопасности	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности.	
3.	Защита информации	Использование защищенных компьютерных систем. Методы криптографии Основные технологии построения защищенных систем. Место информационной безопасности экономических систем в национальной безопасности страны.	

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Университет Иннополис обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечной системе (электронной библиотеке) и к электронной информационно-образовательной среде Университета (<https://my.university.innopolis.ru>). Электронно-библиотечная система

и электронная информационно-образовательная среда обеспечивают возможность доступа, обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет»), как на территории Университета, так и вне его.

Также обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам.

Перечень учебно-методического обеспечения дисциплины (модуля):

Основная литература:

1. Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей: учебное пособие / В. Н. Костин. — Москва: Издательский Дом МИСиС, 2018. — 31 с. — Режим доступа: <http://www.iprbookshop.ru/98200.html> — ЭБС «IPRbooks».
2. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — 3-е изд. — Саратов : Профобразование, 2024. — 446 с. — Режим доступа: <https://www.iprbookshop.ru/145915.html> — ЭБС «IPRbooks».
3. Singh, A. K, Mohan, A. Handbook of Multimedia Information Security: Techniques and Applications. — Publishing House: Springer Nature Switzerland, 2019. — 808 p. — Режим доступа: <https://link.springer.com/book/10.1007/978-3-030-15887-3> — Полнотекстовая англоязычная БД Springer.

Дополнительная литература:

1. Артемов, А. В. Информационная безопасность: курс лекций / А. В. Артемов. — Орел: Межрегиональная Академия безопасности и выживания (МАБИБ), 2014. — 256 с. — Режим доступа: <http://www.iprbookshop.ru/33430.html> — ЭБС «IPRbooks».
2. Гулятьева, Т. А. Основы информационной безопасности: учебное пособие / Т. А. Гулятьева. — Новосибирск: Новосибирский государственный технический университет, 2018. — 79 с. — Режим доступа: <http://www.iprbookshop.ru/91640.html> — ЭБС «IPRbooks».
3. Biffi, S., Eckhart, M., Lüder, A., Weippl E. Security and Quality in Cyber-Physical Systems Engineering. — Publishing House: Springer Nature Switzerland, 2019. — 507 p. — Режим доступа: <https://link.springer.com/book/10.1007/978-3-030-25312-7> — Полнотекстовая англоязычная БД Springer.

Дистанционная поддержка дисциплины (модуля)

Для дистанционной поддержки дисциплины используется система управления образовательным контентом Moodle, развернутая на портале АНО ВО «Университет Иннополис». Во время обучения все студенты получают индивидуальные пароли для входа в систему, в которой размещаются: программа курса, контрольные вопросы, задания, темы лекций с презентационными материалами и т. д.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

1. Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведе-

ние всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

2. Специальные помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины обеспечивается в учебных аудиториях, оснащенных:

- столами и стульями;
- компьютерной техникой;
- специализированным оборудованием, включая демонстрационное оборудование.

Перечень материально-технического оснащения учебных аудиторий конкретизируется приказом директора или уполномоченного им лица ежегодно и размещается на официальном сайте Университета в информационно-коммуникационной сети «Интернет» в подразделе «Материально-техническое обеспечение и оснащённость образовательного процесса. Доступная среда» раздела «Сведения об образовательной организации» по ссылке: <https://innopolis.university/sveden/objects>.

3. Для проведения занятий лекционного и семинарского (практического) типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие программе дисциплины (модуля).

4. Лаборатории Университета, в том числе Кибер-физическая лаборатория информационной безопасности «Иннокиберполигон» (<https://engineerschool.innopolis.university/innocyberpolygon>), Цифровая лаборатория искусственного интеллекта «InnoDataHub» (<https://engineerschool.innopolis.university/innodatahub>), Цифровая образовательная песочница для разработки передовых систем «DevOps Playground» (<https://engineerschool.innopolis.university/devops>), оснащены лабораторным и специализированным оборудованием. Перечень материально-технического оснащения и программного обеспечения лабораторий размещается на официальном сайте Университета по ссылке: <https://innopolis.university/sveden/objects>.

5. Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к в электронную информационно-образовательную среду Университета.

6. Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
Электронно-библиотечные системы:			
1.	http://www.iprbookshop.ru	Русскоязычная ЭБС на платформе «IPR Smart». Учебники и учебные пособия для университетов издательства «IPRbooks». Учебники и учебные пособия для лиц с ОВЗ	Индивидуальный неограниченный доступ
2.	http://e.lanbook.com	Русскоязычная ЭБС на платформе «Лань». Учебники и учебные пособия для университетов издательства «Лань». Учебники и учебные пособия для лиц с ОВЗ	Индивидуальный неограниченный доступ
Профессиональные базы данных:			
3.	http://search.ebscohost.com	Платформа EBSCOHost. Доступ к англоязычным полнотекстовым книгам	Индивидуальный неограниченный доступ
4.	https://portal.university.innopolis.ru/reading_hall	Электронный каталог научно-технической библиотеки АНО ВО «Университет Иннополис»	Для студентов, зарегистрированных в системе
5.	https://habr.com	База данных для IT-специалистов	Доступ свободный
6.	https://www.sciencedirect.com	База данных ScienceDirect	Доступ свободный
7.	https://elibrary.ru	Научная электронная библиотека	Доступ свободный
8.	https://link.springer.com	Полнотекстовая англоязычная БД Springer	Доступ из локальной сети УИ. Для удаленного доступа требуется регистрация из локальной сети УИ
9.	https://ar.cnki.net	База Данных Academic Reference. База данных полнотекстовых англоязычных ресурсов по всем академическим дисциплинам, опубликованных в Китае	Доступ из локальной сети УИ
10.	https://www.ams.org/journals	База данных англоязычных полнотекстовых журналов AMS Journals (2017–2022 гг.)	Доступ из локальной сети УИ
11.	https://www.dl.begellhouse.com/collections/6764f0021c05bd10.html	База данных англоязычных полнотекстовых журналов Begell	Доступ из локальной сети УИ
12.	https://saemobilus.sae.org/	База данных англоязычных полнотекстовых журналов SAE International SAE eJournals eBooks	Доступ из локальной сети УИ
13.	https://www.worldscientific.com	База данных англоязычных полнотекстовых журналов WorldScientific 2001–2022 гг.	Доступ из локальной сети УИ
14.	https://www.scitation.org/ebooks	AIPP E-Book Collection I + Collection II. Англоязычная База данных полнотекстовых электронных книг.	Доступ из локальной сети УИ
15.	https://ufn.ru/	Автономная некоммерческая организация Редакция журнала "Успехи физических наук". Электронный журнал на русском языке.	Доступ из локальной сети УИ
16.	https://sk.sagepub.com/book/discipline	SAGE Publications Ltd eBook Collections. Англоязычная База данных полнотекстовых электронных книг	Доступ из локальной сети УИ
17.	https://onlinelibrary.wiley.com/	The Wiley Journals Database Англоязычная База данных полнотекстовых электронных журналов	Доступ из локальной сети УИ
18.	https://www.mathnet.ru/	Полнотекстовая коллекция русскоязычных электронных математических журналов	Доступ из локальной сети УИ

19.	https://quantum-electron.lebedev.ru/arhiv/	Электронная версия журнала «Квантовая электроника»	Доступ из локальной сети УИ
20.	http://journals.rcsi.science/	Полнотекстовая коллекция журналов Российской академии наук включает 140 наименований журналов, охватывающих различные научные специальности.	Доступ из локальной сети УИ
21.	https://www.orbit.com/	База данных патентного поиска, объединяющая информацию о более чем 122 миллионах патентных публикаций, полученную из 120 международных патентных ведомств, включая Роспатент, Всемирную организацию интеллектуальной собственности (ВОИС), Европейскую патентную организацию.	Доступ из локальной сети УИ
Информационные справочные системы:			
22.	https://minobrnauki.gov.ru/	Официальный сайт Министерства науки и высшего образования Российской Федерации	Доступ свободный
23.	https://www.edu.ru/	Федеральный портал «Российское образование»	Доступ свободный
24.	http://window.edu.ru/	Информационная система "Единое окно доступа к образовательным ресурсам"	Доступ свободный
25.	http://school-collection.edu.ru/	Единая коллекция цифровых образовательных ресурсов	Доступ свободный
26.	http://fcior.edu.ru/	Федеральный центр информационно-образовательных ресурсов	Доступ свободный

7. Университет Иннополис обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, в который входят:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		
Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		
КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Системы управления обучением:		
Система LMS Moodle	зарубежное	свободно распространяемое
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное

Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое
Bash (Unix shell)	зарубежное	свободно распространяемое
Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. МЕТОДИЧЕСКИЕ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Задания для семинарских (практических) занятий:

№ п/п	Наименование раздела дисциплины (модуля)	Перечень рассматриваемых тем (вопросов)
1.	Основополагающие положения	Практические задания на семинарских занятиях: 1. Составление блок-схемы «Классификация угроз в АСОД». 2. Составление блок-схемы «Классификация механизмов защиты информации». 3. Работа с программами для раскрытия пароля. 4. Сниффинг пакетов.
2.	Основные положения теории информационной безопасности	Практические задания на семинарских занятиях: 1. Анализ способов нарушений информационной безопасности. 2. Составление таблицы «Программно-технические изделия, предназначенные для защиты информации в ПК». 3. Составление блок-схемы «Классификация вредоносных программ». 4. Меры по устранению угрозы IP – спуфинга. 5. Механизмы защиты для обеспечения конфиденциальности данных и сообщений.
3.	Защита информации	Разработка отдельных частей кода программного продукта: 1. Методы криптографии. 2. Основные технологии построения защищенных систем. 3. Механизмы защиты для обеспечения идентификации и аутентификации пользователей. 4. Дифференциальный криптоанализ. 5. Симметричная и асимметричная криптосистема.

Текущий контроль успеваемости обучающихся по дисциплине (модулю):

№ п/п	Наименование раздела дисциплины (модуля)	Форма текущего контроля	Материалы текущего контроля
1.	Основополагающие положения	Проверка выполнения домашних зада-	Устный / письменный опрос: 1. Понятие угрозы. 2. Информационная безопасность в условиях функционирова-

		ний; Устный / письменный опрос; Тестирование (письменное или компьютерное)	ния в России глобальных сетей 3. Понятие о видах вирусов Тестирование: 1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется. Выберите один ответ. - Компилятор - Интернет-черви - Вирус 2. величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется Выберите один ответ. - Воздействием (влиянием) - Потерей - Силой 3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется Выберите один ответ. - Троянской программой - Червем - Вирусом
2.	Основные положения теории информационной безопасности	Проверка выполнения домашних заданий; Устный / письменный опрос; Тестирование (письменное или компьютерное); Доклад; Защита проекта; Проверка разработки отдельных частей кода программного продукта	Устный / письменный опрос: 1. Задачи в сфере обеспечения информационной безопасности на уровне государства 2. Модели безопасности и их применение. 3. Причины, обуславливающие существование нарушения безопасности. 4. Способов нарушений информационной безопасности. Тестирование 1. Системные файлы, обеспечивающие поддержку структур файловой системы, называются: Выберите один ответ. - Каталоги - Символьные файлы - Регулярные файлы 2. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются Выберите один ответ. - Вирусами - Руткитами - Червями 3. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется: Выберите один ответ. - Правилами безопасности - Требованием безопасности - Мерами безопасности 4. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

			Выберите один ответ. - Управление риском - Предупреждением рисков - Анализом рисков Задания, в том числе, для групповых проектов: 1. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
3.	Защита информации	Проверка выполнения домашних заданий; Устный / письменный опрос; Тестирование (письменное или компьютерное); Защита проекта	Устный / письменный опрос: 1. Перечислите основные методы криптографии 2. Современные средства защиты информации 3. Современные системы компьютерной безопасности 4. Какая компьютерная система является защищенной Задания, в том числе, для групповых проектов: 1. Атаки на систему безопасности и современные методы защиты Тестирование: 1. Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется Выберите один ответ. - Мультипроцессоры типа «хозяин-подчиненный» - Симметричный мультипроцессор - Мультипроцессор с общей памятью

Контрольные вопросы для подготовки к промежуточной аттестации:

№ п/п	Наименование раздела дисциплины (модуля)	Наименование вопроса
1.	Основополагающие положения	Что такое информационная безопасность? Какие предпосылки и цели обеспечения информационной безопасности? В чем заключаются национальные интересы РФ в информационной сфере? Что включает в себя информационная борьба? Какие пути решения проблем информационной безопасности РФ существуют? Каковы общие принципы обеспечения защиты информации? Какие имеются виды угроз информационной безопасности предприятия (организации)? Какие источники наиболее распространенных угроз информационной безопасности существуют? Какие виды сетевых атак имеются?
2.	Основные положения теории информационной безопасности	Что включает борьба с атаками на уровне приложений? Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей? В чем заключается распределенное хранение файлов? Что включают в себя требования по обеспечению комплексной системы информационной безопасности? Какие уровни информационной защиты существуют, их основные составляющие? В чем заключается контроль участников взаимодействия? Какие функции выполняет служба регистрации и наблюдения? Что такое информационно-опасные сигналы, их основные параметры? Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники? Какой процесс называется аутентификацией пользователя?

3.	Защита информации	В чем заключаются задачи криптографии? Зачем нужны ключи? Какая схема шифрования называется многоалфавитной подстановкой? Какие системы шифрования вы знаете? Что включает в себя защита информации от несанкционированного доступа? В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации? Какие задачи выполняет подсистема управления доступом? Какие требования предъявляются к подсистеме протоколирования аудита? Какие схемы аутентификации вы знаете? Что такое смарт-карты?
----	-------------------	---

Вопросы/Задания к промежуточной аттестации в устной/письменной форме:

1. Международные стандарты информационного обмена.
2. Виды противников или «нарушителей».
3. Классификация механизмов защиты информации.
4. Три вида возможных нарушений информационной системы. Защита.
5. Сниффинг пакетов.
6. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
7. Меры по устранению угрозы IP – спуфинга.
8. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
9. Основные положения теории информационной безопасности. Модели безопасности и их применение.
10. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
11. Механизмы защиты для обеспечения конфиденциальности данных и сообщений.
12. Анализ способов нарушений информационной безопасности.
13. Использование защищенных компьютерных систем.
14. Методы криптографии.
15. Основные технологии построения защищенных систем.
16. Механизмы защиты для обеспечения идентификации и аутентификации пользователей.
17. Дифференциальный криптоанализ.
18. Симметричная криптосистема.
19. Асимметричная криптосистема.

Критерии оценивания сформированности компетенций

Оценивание уровня учебных достижений, обучающихся по дисциплине (модулю), осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

В рамках внутренней системы оценки качества образовательной деятельности по программе обучающимся предоставляется возможность оценивания усло-

вий, содержания, организации и качества образовательного процесса по данной дисциплине (модулю).

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме экзамена, при этом проводится оценка компетенций, сформированных по дисциплине.

Система оценивания результатов обучения по дисциплине (модулю)

Знания, умения и навыки обучающихся при промежуточной аттестации определяются в следующей форме: «отлично» (А), «хорошо» (В), «удовлетворительно» (С), «неудовлетворительно» (D).

Критерии оценивания результатов обучения по дисциплине (модулю)

Результат обучения по дисциплине (модулю)	Общая характеристика результата обучения по дисциплине (модулю)
А «Отлично»	Обучающийся владеет знаниями предмета в полном объеме рабочей программы, достаточно глубоко осмысливает дисциплину; самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивая при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи; четко формирует ответы, свободно читает результаты анализов и других исследований и решает ситуационные задачи повышенной сложности; хорошо знаком с основной литературой и методами исследования большого объема, необходимым для практической деятельности; увязывает теоретические аспекты предмета с задачами практического значения.
В «Хорошо»	Обучающийся владеет знаниями предмета практически в полном объеме рабочей программы; самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивая при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи; четко формирует ответы, свободно читает результаты анализов и других исследований и решает ситуационные задачи повышенной сложности; хорошо знаком с основной литературой и методами исследования большого объема, необходимым для практической деятельности; увязывает теоретические аспекты предмета с задачами практического значения.
С «Удовлетворительно»	Обучающийся владеет основным объемом знаний по дисциплине; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов. Обучающийся способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований.
D «Неудовлетворительно»	Обучающийся не освоил обязательного минимума знаний предмета, не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

Методические указания для обучающихся по освоению дисциплины (модуля)

Вид учебных занятий/деятельности	Деятельность обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения лекции, выводы, формулировки, обобщения; пометать важные мысли, выделять ключевые слова, термины. Обозначить вопросы, термины или другой материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в

	материале, необходимо сформулировать вопрос и задать преподавателю на консультации, во время семинарского (практического) занятия.
Практическое (семинарское) занятие	При подготовке к семинарскому (практическому) занятию необходимо проработать материалы лекций, основной и дополнительной литературы по заданной теме. На основании обработанной информации постараться сформировать собственное мнение по выносимой на обсуждение тематике. Обосновать его аргументами, сформировать список источников, подкрепляющих его. Во время семинарского (практического) занятия активно участвовать в обсуждении вопросов, высказывать аргументированную точку зрения на проблемные вопросы. Приводить примеры из источниковой базы и научной и/или исследовательской литературы.
Устный/письменный опрос	Отвечать, максимально полно, логично и структурировано, на поставленный вопрос. Основная цель – показать всю глубину знаний по конкретной теме или ее части.
Подготовка к промежуточной аттестации	При подготовке к промежуточной аттестации необходимо проработать вопросы по темам, которые рекомендуются для самостоятельной подготовки. При возникновении затруднений с ответами следует ориентироваться на конспекты лекций, семинаров, рекомендуемую литературу, материалы электронных и информационных справочных ресурсов, статей. Если тема вызывает затруднение, четко сформулировать проблемный вопрос и задать его преподавателю.
Практические (лабораторные) занятия	Практические занятия предназначены прежде всего для разбора отдельных сложных положений, тренировки аналитических навыков, а также для развития коммуникационных навыков. Поэтому на практических занятиях необходимо участвовать в тех формах обсуждения материала, которые предлагает преподаватель: отвечать на вопросы преподавателя, дополнять ответы других студентов, приводить примеры, задавать вопросы другим выступающим, обсуждать вопросы и выполнять задания в группах. Работа на практических занятиях подразумевает домашнюю подготовку и активную умственную работу на самом занятии. Работа на практических занятиях в форме устного опроса заключается прежде всего в тренировке навыков применять теоретические положения к самому разнообразному материалу. В ходе практических занятий студенты работают в группах для обсуждения предлагаемых вопросов.
Самостоятельная работа	Самостоятельная работа состоит из следующих частей: 1) чтение учебной, справочной, научной литературы; 2) повторение материала лекций; 3) составление планов устных выступлений; 4) подготовка видеопрезентации. При чтении учебной литературы нужно разграничивать для себя материал на отдельные проблемы, концепции, идеи. Учебную литературу можно найти в электронных библиотечных системах, на которые подписан АНО Университет Иннополис.
Доклад	Публичное, развернутое сообщение по определенной теме или вопросу, основанное на документальных данных. При подготовке доклада рекомендуется использовать разнообразные источники, позволяющие глубже разобраться в теме. Учебную литературу можно найти в электронных библиотечных системах, на которые подписан АНО Университет Иннополис.
Дискуссия	Публичное обсуждение спорного вопроса, проблемы. Каждая сторона должна оппонировать мнение собеседника, аргументируя свою позицию.
Тестирование (устное/письменное)	При подготовке к тестированию необходимо проработать материалы лекций, семинаров, основной и дополнительной литературы по заданной теме. Основная цель тестирования – показать уровень сформированности знаний по конкретной теме или ее части.
Разработка отдельных частей кода	Разработать часть кода, исходя из поставленной задачи и рекомендаций преподавателя. При выполнении работы рекомендуется обращаться к материалам лекций

	и семинарских (практических) занятий. Если возникают затруднения, необходимо проконсультироваться с преподавателем.
Выполнение домашних заданий и групповых проектов	Для выполнения домашних заданий и групповых проектов необходимо получить формулировку задания от преподавателя и убедиться в понимании задания. При выполнении домашних заданий и групповых проектов необходимо проработать материалы лекций, основной и дополнительной литературы по заданной теме.

Для подготовки к занятиям рекомендуется использовать представленные источники в электронных форматах и дополнительную литературу.

8. ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

Данная программа и/или ее фрагменты не могут быть использованы другими образовательными организациями без соответствующего разрешения АНО ВО «Университет Иннополис».