

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

Кафедра информационных технологий

Утверждаю
Зав. кафедрой
О.В.Федорова
Протокол заседания
кафедры № 10
от 06.04.2026

Рабочая программа дисциплины

Наименование дисциплины	Разработка безопасных систем
Направление подготовки	09.03.01 Информатика и вычислительная техника
Направленность (профиль) образовательной программы	Инженерия информационных систем
Год набора	2025, 2026

Составители:

Старший преподаватель магистерской программы «Разработка безопасных сетей и систем» Салтанов К. 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 единицах	академических часах	Лекции, час.	Семинарские (практические) занятия, час.			
очная	8	4	144	30	30	9	75	экзамен

1. КРАТКАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ (МОДУЛЯ)

Изучение дисциплины (модуля) «Secure System Development / Разработка безопасных систем» обеспечивает формирование и развитие компетенций обучающихся в области разработки безопасных систем, их применение для решения различных прикладных задач в рамках профессиональной деятельности. В ходе освоения дисциплины обучающиеся рассматривают виды и компоненты систем защиты информации, способы их развертывания и настройки, основные угрозы, уязвимости, защитные меры, вектора атак на как на отдельные компоненты, узлы, так и на всю инфраструктуру целевой организации, методологии и лучшие практики проведения тестирования на проникновения, оценки защищенности целевой системы.

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 предоставление обучаемым знаний и умений в области проектирования, разработки, тестирования, отладки, внедрения и сопровождения программного обеспечения вычислительной техники.

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	Индикаторы компетенций	Методы и технологии обучения, способствующие формированию компетенции
1.	ПК-1	Способен разрабатывать требования и проектировать программное обеспечение, создавать и поддерживать среды разработки, автоматизировать и контролировать	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 программного	Метод дискуссии; Метод контрольных вопросов; Проектная технология; Информационно – коммуникационная технология; Групповая технология

		качество разработки программных решений для информационных систем	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-4	Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения информационных систем	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; регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе; требования охраны труда при работе с сетевой аппаратурой информационной	Метод дискуссии; Метод контрольных вопросов; Проектная технология; Информационно – коммуникационная технология; Групповая технология

			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 использование российских программных решений и решений с открытым исходным кодом; решать задачи по деплою под разные языки программирования и платформы; выбирать и настраивать необходимые сервисы 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 об основных видах и компонентах систем защиты информации, способах их развертывания и настройки; основных угрозах, уязвимости, защитных мерах, о векторе атак как на отдельные компоненты, узлы, так и на всю инфраструктуру целевой организации; о методологии и практиках проведения тестирования на проникновения, оценки защищенности целевой системы; о проблемах, с которыми сталкиваются технологии обеспечения информационной безопасности мобильных операционных систем; о технологии обеспечения информационной безопасности баз данных; о методах разработки безопасного программного обеспечения, способах эксплуатации и способах защиты, которые могут затрагивать как непосредственно логику программного кода, особенности языка программирования, так и операционной системы, под которую разрабатывается приложение.

Умения: сформированы умения использовать различное открытое программное и программно-аппаратное обеспечение для создания защищенных систем, а также проводить тестирование безопасности, их компонентов и разрабатывать рекомендации по улучшению с точки зрения информационной безопасности на этой основе; проводить анализ защищенности мобильных операционных систем и приложений; администрировать различные технологии баз данных с точки зрения информационной безопасности; разрабатывать безопасное программное обеспечение, искать низкоуровневые уязвимости в открытом исходном коде, создавать программный код, использующий уязвимости в программном обеспечении, и вырабатывать меры по повышению безопасности кода программ; проводить тестирование защищенности программных продуктов статическим, динамическим анализом: методом белого, серого, черного ящика; разработать рекомендации по улучшению степени защищенности инфраструктуры или отдельного продукта, по которому проводился анализ защищенности, реализация которых не приведет к потере производительности, непрерывности бизнес-процессов или иным репутационным рискам для организации.

Навыки (владения): сформировано владение навыками по развертыванию и обслуживанию компонентов, которые отвечают за обеспечение защищенности инфраструктуры; навыками по использованию готовых решений или разработке собственных для тестирования защищенности компонентов; навыками по автоматизации тестирований защищенности, аудита безопасности и т.д.; навыками по использованию лучших практик для проведения оценки защищенности продукта, инфраструктуры; навыками по использованию актуальных практик в разработке безопасного программного обеспечения.

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) «Secure System Development / Разработка безопасных систем» 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 8 семестре.

4. ОБЪЕМ, СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) составляет:

4 зачетные единицы, 144 академических часа, 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.	Безопасность сетевой инфраструктуры	6	6	0	18
2.	Безопасность ПО	8	8	0	19
3.	Безопасность баз данных	8	8	0	19

4.	Разработка безопасного ПО	8	8	0	19
	Промежуточная аттестация - экзамен			9	
ИТОГО:		30	30	9	75

Содержание дисциплины (модуля):

№ раздела	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам	Формируемые компетенции
1.	Безопасность сетевой инфраструктуры	Основные угрозы сетевой инфраструктуры организации. Межсетевые экраны. Основные методики построения систем противодействия угрозам сетевого уровня. Вероятностная модель расчета успешности проведения атаки. Методы оптимизации производительности систем противодействия угрозам сетевого уровня.	ПК-1; ПК-4
2.	Безопасность ПО	Основы безопасности ПО. Основные угрозы и уязвимости приложений. Методологии и лучшие практики обнаружения уязвимостей. Классификаторы. Методики проведения комплексной оценки защищенности ПО.	
3.	Безопасность баз данных	Основы безопасности баз данных. Методы обеспечения информационной безопасности баз данных.	
4.	Разработка безопасного ПО	Обзор методик разработки безопасного ПО на каждом ее этапе. Техники тестирования. Методы защиты и поиска уязвимостей в коде.	

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. Компьютерные сети: учебно-методический комплекс / составители О. С. Ахметова, А. Опабекова, А. М. Сатымбеков. — Алматы: Нур-Принт, 2012. — 295 с. — Режим доступа: <http://www.iprbookshop.ru/67067.html> — ЭБС «IPRbooks».
2. Шелухин, О. И. Системы обнаружения вторжений в компьютерные сети: учебное пособие / О. И. Шелухин, А. Н. Руднев, А. В. Савелов. — Москва: Московский технический университет связи и информатики, 2013. — 88 с. — Режим доступа: <http://www.iprbookshop.ru/63360.html> — ЭБС «IPRbooks».

Дополнительная литература:

1. Синицын, С. В. Верификация программного обеспечения: учебное пособие / С. В. Синицын, Н. Ю. Налютин. — 3-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 367 с. — Режим доступа: <https://www.iprbookshop.ru/97540.html> — ЭБС «IPRbooks».
2. Ракитин, Р. Ю. Компьютерные сети: учебное пособие / Р. Ю. Ракитин, Е. В. Москаленко. — Барнаул: Алтайский государственный педагогический университет, 2019. — 338 с. — Режим доступа: <http://www.iprbookshop.ru/102731.html> — ЭБС «IPRbooks».
3. Tanenbaum, Andrew S. Computer Networks 5th. — Publishing House: Pearson Education Limited, 2015. — 960 p. — Режим доступа: https://portal.university.innopolis.ru/reading_hall/detail.php?ID=99843 — Электронный каталог научно-технической библиотеки АНО ВО «Университет Иннополис».

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

2. 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. 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 оснащенность 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/books/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.	Безопасность сетевой инфраструктуры	Объединитесь с кем-нибудь в команду и выполните задание в соответствии с пунктами ниже: 1. Разработать план по аудиту и поиску уязвимостей в предоставленном шаблоне типовой инфраструктуры предприятия. 2. Выявить уязвимости, разработать рекомендации по устранению. Написать отчет о проделанной работе.
2.	Безопасность ПО	Объединитесь с кем-нибудь в команду и выполните задание в соответствии с пунктами ниже: 1. Проанализировать предоставленное ПО на уязвимости методом черного ящика. 2. Разработать соответствующие эксплойты и провести атаку Написать отчет о проделанной работе.
3.	Безопасность баз данных	Объединитесь с кем-нибудь в команду и выполните задание в соответствии с пунктами ниже: 1. Разработать план по аудиту и поиску уязвимостей в предоставленном шаблоне СУБД. 2. Выявить уязвимости, разработать рекомендации по устранению Написать отчет о проделанной работе.
4.	Разработка безопасного ПО	Объединитесь с кем-нибудь в команду и выполните задание в соответствии с пунктами ниже: 1. Проанализировать предоставленное ПО на уязвимости методом черного ящика открытого исходного кода. 2. Разработать соответствующие эксплойты и провести атаку. 3. Разработать рекомендации по устранению найденных уязвимостей. Написать отчет о проделанной работе.

Текущий контроль успеваемости обучающихся по дисциплине (модулю):

№ п/п	Наименование раздела дисциплины (модуля)	Форма текущего контроля	Материалы текущего контроля
1.	Безопасность сетевой	Проверка	Темы групповых проектов:

	инфраструктуры	выполнения домашних заданий; Устный / письменный опрос; Доклад; Защита проекта; Коллоквиум	На примере типовой инфраструктуры организации найти угрозы сетевой безопасности. Сделайте отчет Осуществить сетевое вторжение. Обойти системы обнаружения; сделать отчет Перехватить трафик используя Sniffing. Групповая практическая работа: осуществить сетевую атаку методом подбора пароля. Групповая практическая работа: использовать готовый rootkit для сбора данных в закрытой сети.
2.	Безопасность ПО	Проверка выполнения домашних заданий; Устный / письменный опрос; Доклад; Защита проекта; Контрольная работа	Темы групповых проектов: Осуществите попытки осуществления взлома web мобильного приложения, злоупотребляя реальными недостатками. Возможно использование SQL-инъекции, либо межсайтовый скриптинг. Подготовить отчет о результатах. В готовом веб-приложении необходимо выбрать уязвимость и с помощью нее осуществить взлом. Подготовить отчет и возможность убрать данную уязвимость. Групповая контрольная работа: Используя различные методики провести комплексную оценку защищенности инфраструктуры веб-приложений
3.	Безопасность баз данных	Проверка выполнения домашних заданий; Устный / письменный опрос; Доклад; Защита проекта; Контрольная работа	Темы групповых проектов: Осуществите попытки осуществления взлома web и мобильного приложения, злоупотребляя реальными недостатками. Возможно использование SQL-инъекции, либо межсайтовый скриптинг. Подготовить отчет о результатах. В готовом веб-приложении необходимо выбрать уязвимость и с помощью нее осуществить взлом. Подготовить отчет и возможность убрать данную уязвимость. Групповая контрольная работа: Используя различные методики провести комплексную оценку защищенности инфраструктуры веб-приложений.
4.	Разработка безопасного ПО	Проверка выполнения домашних заданий; Устный / письменный опрос; Доклад; Защита проекта	Темы групповых проектов: Проанализируйте ПО, установленное в вашей системе. 1. Анализ ПО Попытайтесь исследовать какое-либо ПО и изучить, что оно делает. 1) Используйте песочницы для определения того, что делает это ПО. 2) Можете ли вы применить reverse engineering по отношению программе? 3) Какие функционал ПО? 2. Malware signature Используя Clam-AV у вас есть возможность написать свои собственные правила вредоносного ПО. 1) Какие существуют правила подписи? 2) Проанализируйте поведение вредоносного ПО. 3) Создайте логическую подпись для этого. 5. Полиморфное вредоносное ПО. Вредоносные программы могут обнаруживаться вирусными сканерами, но есть некоторые ограничения. 1) Какие инструменты используются для полиморфизма вредоносных программ? 2) Как работают эти инструменты?

			3) Изменяют ли эти пакеты поведение вредоносного ПО? 3. Crypto malware. Существует множество криптозащитных программ. 1) Создайте вредоносное ПО PoC с использованием любого языка программирования, который работает в пользовательском пространстве. 2) Используйте различные методики, чтобы проанализировать ваше программное обеспечение
--	--	--	--

Контрольные вопросы для подготовки к промежуточной аттестации:

№ п/п	Наименование раздела дисциплины (модуля)	Наименование вопроса
1.	Безопасность сетевой инфраструктуры	Опишите основные свойства беспроводных технологий коммуникации. С какими основными типами вы знакомы? Приведите примеры основных технологий и опишите их специфику. Объясните принцип построения защищенных беспроводных сетей. Как осуществляется обнаружение незаконных передач.
2.	Безопасность ПО	Каким образом основные принципы по осуществлению безопасности будут работать в NoSQL? Как это повлияет на производительность? Какие типы уязвимостей используются для атак на Android устройства? Опишите архитектуру Android с позиции осуществления безопасности. Техники написания эксплойтов.
3.	Безопасность баз данных	Назовите основные принципы безопасности базы данных. В чем заключается специфика приема по шифрованию базы данных? Укажите основные уровни безопасности данных. Назовите основные параметры аутентификации пользователя.
4.	Разработка безопасного ПО	Опишите инструментальные программные средства (ИПС) создания программ, выполняемых на стороне сервера. В чем разница между Docker Image и Docker Container. Их характеристика и назначение. Основные моменты работы blockchain. Криптозащитные программы. Приведите примеры основных. Опишите принцип и значение работы программ. Вирусные сканеры. Принцип их работы. Устройство сканеров.

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

1. Осуществите попытки осуществления взлома web мобильного приложения, злоупотребляя реальными недостатками. Возможно использование SQL-инъекции, либо межсайтовый скриптинг. Подготовить отчет о результатах.
2. В готовом веб-приложении необходимо выбрать уязвимость и с помощью нее осуществить взлом. Подготовить отчет и возможность убрать данную уязвимость.

3. Осуществите попытки осуществления взлома web и мобильного приложения, злоупотребляя реальными недостатками. Возможно использование SQL-инъекции, либо межсайтовый скриптинг. Подготовить отчет о результатах.
4. Используя Clam-AV, у вас есть возможность написать свои собственные правила вредоносного ПО.
 - 1) Какие существуют правила подписи?
 - 2) Проанализируйте поведение вредоносного ПО.
 - 3) Создайте логическую подпись для этого.
5. Создайте вредоносное ПО PoC с использованием любого языка программирования, который работает в пользовательском пространстве.
6. Разработать план по аудиту и поиску уязвимостей в предоставленном шаблоне типовой инфраструктуры предприятия. Выявить уязвимости, разработать рекомендации по устранению. Написать отчет о проделанной работе.
7. Разработать план по аудиту и поиску уязвимостей в предоставленном шаблоне СУБД. Выявить уязвимости, разработать рекомендации по устранению. Написать отчет о проделанной работе.

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 условий, 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; пометить 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, подтверждающих 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 мнению собеседника, аргументируя свою позицию.
Контрольная работа	При подготовке к контрольной работе необходимо проработать материалы лекций, семинаров, основной и дополнительной литературы по заданной теме.
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».