МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. директора института перспективной инженерии
_____ А.А.Порохня

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Кибербезопасность

Направление подготовки	09.03.04 Программная инженерия
Направленность (профиль)	Инженерия сложных программных систем
Форма обучения	очная
Год начала обучения	2026
Реализуется в	8 семестре

Разработал
Ассистент межинститутской базовой кафедры департамента цифровых, робототехнических систем и электроники
Потапов И.Р.

Ставрополь 2026 г.

1. Цели и задачи освоения дисциплины (модуля)

Целью освоения дисциплины «Кибербезопасность» является формирование у студентов компетенции по практической защите программных систем от кибератак, управлению инцидентами, тестированию на проникновение, а также по разработке нормативной документации в области кибербезопасности.

Задачи дисциплины:

1. Изучить жизненный цикл кибератаки (MITRE ATT&CK) и методы противодействия.
2. Освоить технологии мониторинга, обнаружения и реагирования на инциденты (SIEM, SOAR).
3. Научиться проводить тестирование на проникновение (пентест) и анализ защищенности.
4. Развить навыки разработки документов: регламент реагирования, акт тестирования, план непрерывности.
5. Обеспечить соблюдение требований ПК-10 в условиях активных угроз.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Кибербезопасность» относится к части, формируемой участниками образовательных отношений Блока 1 (Б1.В.05). Ее освоение происходит в 8 семестре.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

3.1 Наименование компетенций

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-10 – Готов соблюдать правовые нормы, стандарты и требования информационной безопасности, участвовать в разработке нормативной и технической документации, учитывать законодательство в области ИТ	ИД-1$_{ПК-10}$ Применяет основные правовые нормы (лицензирование ПО, авторское право, ФЗ-152, ФЗ-149) и стандарты ИБ (ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 56545-2015) при разработке и эксплуатации ПО	Знает методы выявления и анализа инцидентов ИБ, процедуры реагирования, нормативные требования к управлению инцидентами
	ИД-2$_{ПК-10}$ Реализует меры защиты информации: аутентификацию (JWT, OAuth2), авторизацию (RBAC), шифрование, защиту от типовых уязвимостей OWASP Top 10 (SQL-инъекции, XSS, CSRF, IDOR) с учётом требований регуляторов (ФСТЭК)	Умеет применять стандарты и правовые нормы при проведении пентестов, анализе уязвимостей, оформлении актов и отчетов

	ИД-3$_{ПК-10}$ Разрабатывает нормативную и техническую документацию по информационной безопасности: политики парольной защиты, модели угроз, технические задания на подсистему ИБ, инструкции пользователя, регламенты реагирования на инциденты	Владеет навыками разработки документации по реагированию на инциденты, оценке соответствия системы требованиям кибербезопасности

4. Объем учебной дисциплины (модуля) и формы контроля *

Объем занятий: всего 3 з.е. 108 акад.ч.	ОФО
Контактная работа:	42
Лекции/из них практическая подготовка	14
Лабораторных работ/ из них практическая подготовка	28
Практический занятий/ из них практическая подготовка	–
Самостоятельная работа	66
Формы контроля:	
Зачет с оценкой	8 семестр

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества часов и видов занятий

5.1.Тематический план дисциплины (модуля)

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	Очная форма			Самостоятельная работа, часов
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			
			Лекции	Практические занятия	Лабораторные работы	
7 семестр						
1	Эволюция угроз. Тактики и техники MITRE ATT&CK. От вирусов до APT-групп. Обзор матрицы ATT&CK. Примеры	ПК-10$_{ИД-1}$ ПК-10$_{ИД-2}$ ПК-10$_{ИД-3}$	2	-	4	10

	тактик: Initial Access, Execution, Persistence.					
2	Управление уязвимостями (VM). Жизненный цикл уязвимости. CVE, CVSS, базы данных (NVD, БДУ ФСТЭК). Сканеры уязвимостей (OpenVAS, Nessus).	ПК-10$_{ИД-1}$ ПК-10$_{ИД-2}$ ПК-10$_{ИД-3}$	2	-	4	10
3	SIEM и мониторинг событий. Архитектура SIEM. Сбор логов, корреляция событий. Пример правил корреляции. Взаимодействие с законодательством (хранение логов).	ПК-10$_{ИД-1}$ ПК-10$_{ИД-2}$ ПК-10$_{ИД-3}$	2	-	4	10
4	Реагирование на инциденты (IR). Этапы: подготовка, обнаружение, сдерживание, эрадикация, восстановление, уроки. Роли CERT/CSIRT. Нормативная база (Приказ ФСТЭК № 239).	ПК-10$_{ИД-1}$ ПК-10$_{ИД-2}$ ПК-10$_{ИД-3}$	2	-	4	8
5	Тестирование на проникновение. Виды: Black box, White box, Gray box. Этапы пентеста. Правовые аспекты (договор, разрешение). Стандарты PTES, OWASP.	ПК-10$_{ИД-1}$ ПК-10$_{ИД-2}$ ПК-10$_{ИД-3}$	2	-	4	10
6	Защита CI/CD и DevSecOps. Безопасная сборка, SAST, DAST, SCA. Внедрение безопасности в пайплайн. Compliance as Code.	ПК-10$_{ИД-1}$ ПК-10$_{ИД-2}$ ПК-10$_{ИД-3}$	2	-	4	10
7	BCP и DRP. Киберстрахование. Планы непрерывности и восстановления. Резервное копирование. Требования регуляторов. Роль документации (план действий при ЧС).	ПК-10$_{ИД-1}$ ПК-10$_{ИД-2}$ ПК-10$_{ИД-3}$	2	-	4	8
	ИТОГО за 8 семестр		**14**	**-**	**28**	**66**
	ИТОГО		**14**	**-**	**28**	**66**

6. Фонд оценочных средств по дисциплине

Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю) «Высоконагруженные и распределенные системы» базируется на перечне осваиваемых компетенций с указанием этапов их формирования в процессе освоения дисциплины (модуля). ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций;
- типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений и уровня овладения формируемыми компетенциями в процессе освоения дисциплины.

ФОС является приложением к данной программе дисциплины.

7. Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

Лекционный материал посвящен рассмотрению ключевых, базовых положений курсови разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Лабораторные работы направлены на приобретение опыта практической работы в области распознавания образов.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим и лабораторным занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины, необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для освоениядисциплины (модуля)

8.1.1. Перечень основной литературы:

1. Баланов А. Н., «Защита информационных систем. Кибербезопасность». (СПб.: Лань, 2-е изд., 2025. – 280 с. ISBN 978-5-507-50467-1).

2. Мельников В. П., Клейменов С. А., Петраков А. М., «Информационная безопасность». (Учебное пособие. – ISBN 978-5-7695-1816-4).

3. Зенков А. В., «Информационная безопасность и защита информации». (Учебное пособие для вузов. – 104 с. ISBN 978-5-534-14590-8).

4. Лойко В. И. и др., «Информационная безопасность». (Краснодар: КубГАУ, 2020. – 332 с. ISBN 978-5-907346-50-5).

5. Жуков М. М., Телков А. Ю., Авсентьев А. О., Полухин Д. И., «Основы кибербезопасности: практикум». (Воронеж: Воронежский институт МВД России, 2024. – 142 с.).

8.1.2. Перечень дополнительной литературы

6. Абденов А. Ж. Анализ, описание и оценка функциональных узлов SIEM-системы / А. Ж. Абденов, В. А. Трушин, К. Сулайман. – Новосибирск : Новосибирский государственный технический университет, 2018. – 122 с. – ISBN 978-5-7782-3716-2.

7. Баланов А. Н. Защита информационных систем. Кибербезопасность : учебное пособие / А. Н. Баланов. – 2-е изд., перераб. и доп. – Санкт-Петербург : Лань, 2025. – 280 с. – ISBN 978-5-507-50467-1.

8. Burp Suite : официальный сайт. – URL: https://portswigger.net/burp. – Текст : электронный.

9. Девис Р. Искусство тестирования на проникновение в сеть : практическое руководство / Ройс Дэвис ; пер. с англ. – Москва : ДМК Пресс, 2021. – 310 с. – ISBN 978-5-97060-529-5.

10. Елисеев А. И. Основы тестирования КИИ на проникновение : учебное пособие / А. И. Елисеев, Д. В. Поляков. – Москва : РУДН, 2020. – 120 с. – ISBN 978-5-8265-2090-1.

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

1. GitLab DevSecOps : официальная документация. – URL: https://docs.gitlab.com/ee/user/application_security. – Текст : электронный.

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

При чтении лекции используется компьютерная техника, демонстрация презентационных мультимедийных материалов. На практических работах студенты предоставляют подготовленные ими электронные файлы, выполненных заданий.

Информационные справочные системы:

Информационно-справочные и информационно-правовые системы, используемые приизучении дисциплины:

1.	http://apps.webofknowledge.com – Информационно-аналитическая система «Web of Science»
2.	https://www.scopus.com – Информационно-аналитическая система «Scopus».
3.	https://elibrary.ru/ – Научная электронная библиотека.
4.	https://нэб.рф/ – Национальная электронная библиотека.
5.	https://www.rsl.ru – /Российская государственная библиотека.

Программное обеспечение:

1.	Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). MicrosoftOfficeStandard 2013: договор № 01-эа/13 от 25.02.2013г., Лицензирование Microsoft Office https://support.microsoft.com/ru-ru/lifecycle/search/16674 Дата начала жизненного цикла 09.01.2013г.; набор обновлений Office 2013 Service Pack 1 Дата начала жизненного цикла 25.02.2014г., Дата окончания основной фазы поддержки 10.04
2.	Операционная система: Microsoft Windows 10: 2016-08(20), 2017-10(67), 2018-01(18), 2018-04(6), 2018-05(6), 2019-02(7). Бессрочная лицензия. Договоры № 27-эа/16 от 02.08.2016. и № 0321100021117000009_229123 от 10.10.2017. На текущий момент окончания поддержки не анонсировано
3.	Docker, Docker Compose, Rsyslog, GitLab, Metasploitable 2, SonarQube, Ubuntu

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия	1.	Веб-камера Logitech HD Pro WebcamC920 1920[1080Mic USB
	2.	Короткофокусный мультимедиа-проектор Epson
	3.	Магнитно-маркерные доски белые с эмалевой поверхностью CC MagnetopIan
	4.	Монитор 17" TFT Филипс
	5.	Наушники с микрофономCreativeHS-33051EF0290AA001 накладные,черный/серый
	6.	Перс.супер компьют.+монитор+клав.+мышь+каб.ПкCi7-5930K/8D8192D4-2133/K2200/2K40M
Лабораторные занятия	1.	Веб-камера Logitech HD Pro WebcamC920 1920[1080Mic USB
	2.	Наушники с микрофономCreativeHS-33051EF0290AA001 накладные,черный/серый

	3.	Перс.супер компьют.+монитор+клав.+мышь+каб.ПкCi7-5930K/8D8192D4-2133/K2200/2K40M
Самостоятельная работа	1.	Веб-камераLogitech HD Pro WebcamC920 1920[1080Mic USB
	2.	Монитор 17 TFT" Филипс
	3.	Наушники с микрофономCreativeHS-33051EF0290AA001 накладные,черный/серый
	4.	Перс.супер компьют.+монитор+клав.+мышь+каб.ПкCi7-5930K/8D8192D4-2133/K2200/2K40M

Учебные аудитории для проведения учебных занятий, оснащены оборудованием и техническими средствами обучения. Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде. Специализированная мебель и технические средства обучения, служащие для представления учебной информации.

Материально-техническая база обеспечивает проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, научно-исследовательской работы обучающихся (переносной ноутбук, переносной проектор, компьютеры с необходимым программным обеспечением и выходом в интернет).

11. Особенности освоения дисциплины (модуля) лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,
- специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
- индивидуальное равномерное освещение не менее 300 люкс,
- при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место,

передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;
- обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно- двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента задания могут выполняться в устной форме.

12. Особенности реализации дисциплины с применением дистанционных образовательных технологий и электронного обучения

Согласно части 1 статьи 16 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» под электронным обучением понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. Под дистанционными образовательными технологиями понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Реализация дисциплины может быть осуществлена с применением дистанционных образовательных технологий и электронного обучения полностью или частично. Компоненты УМК дисциплины (рабочая программа дисциплины, оценочные и методические материалы, формы аттестации), реализуемой с применением дистанционных образовательных технологий и электронного обучения, содержат указание на их использование.

При организации образовательной деятельности с применением дистанционных образовательных технологий и электронного обучения могут предусматриваться асинхронный и синхронный способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет».

При применении дистанционных образовательных технологий и электронного обучения в расписании по дисциплине указываются: способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет» (ВКС-видеоконференцсвязь, ЭТ – электронное тестирование); ссылки на электронную информационно-образовательную среду СКФУ, на образовательные платформы и ресурсы иных организаций, к которым предоставляется открытый доступ через информационно-телекоммуникационную сеть «Интернет»; для синхронного обучения - время проведения онлайн-занятий и преподаватели; для асинхронного обучения - авторы онлайн-курсов.

При организации промежуточной аттестации с применением дистанционных образовательных технологий и электронного обучения используются Методические рекомендации по применению технических средств, обеспечивающих объективность результатов при проведении промежуточной и государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры с применением дистанционных

образовательных технологий (Письмо Минобрнаки России от 07.12.2020 г. № МН-19/1573-АН "О направлении методических рекомендаций").

Реализация дисциплины с применением электронного обучения и дистанционных образовательных технологий осуществляется с использованием электронной информационно-образовательной среды СКФУ, к которой обеспечен доступ обучающихся через информационно-телекоммуникационную сеть «Интернет», или с использованием ресурсов иных организаций, в том числе платформ, предоставляющих сервисы для проведения видеоконференций, онлайн-встреч и дистанционного обучения (МТС-Линк), а также с использованием возможностей социальных сетей для осуществления коммуникации обучающихся и преподавателей.

Учебно-методическое обеспечение дисциплины, реализуемой с применением электронного обучения и дистанционных образовательных технологий, включает представленные в электронном виде рабочую программу, учебно-методические пособия или курс лекций, методические указания к выполнению различных видов учебной деятельности обучающихся, предусмотренных дисциплиной, и прочие учебно-методические материалы, размещенные в информационно-образовательной среде СКФУ.