Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.Э.3.1 Защита информации в высокопроизводительных системах»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2026

Рабочая программа дисциплины «*Б1.Д.В.Э.3.1 Защита информации в высокопроизводительных системах*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 9 от "20" марта 2026 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем — И.В. Влацкая
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:

— Ю.Д. Фот
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность — И.В. Влацкая
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
— С.А. Биктимирова
личная подпись *расшифровка подписи*

Уполномоченный по качеству института
— С.Н. Морозова
личная подпись *расшифровка подписи*

№ регистрации _____

© Фот Ю.Д., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: формирование у обучающихся знаний и умений, необходимых для обеспечения защиты информации в высокопроизводительных системах.

Задачи:

Знать:

Основные угрозы безопасности информации в высокопроизводительных системах

Методы и средства защиты информации в высокопроизводительных системах

Нормативно-правовые основы защиты информации

Особенности защиты информации в различных типах высокопроизводительных систем

Уметь:

Разрабатывать и реализовывать комплексные меры защиты информации в высокопроизводительных системах

Использовать методы и средства защиты информации в высокопроизводительных системах

Осуществлять контроль и мониторинг безопасности информации в высокопроизводительных системах

Проводить расследование инцидентов информационной безопасности

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.10 Информатика*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК*-3 Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей	ПК*-3-В-1 Знает основные требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей ПК*-3-В-2 Способен осуществлять разработку и тестирование средств защиты информации компьютерных систем и сетей ПК*-3-В-3 Владеет основными методами защиты информации компьютерных систем и сетей	**Знать:** Основные угрозы безопасности информации в высокопроизводительных системах Программно-аппаратные средства защиты информации в высокопроизводительных системах Нормативно-правовые основы защиты информации Особенности защиты информации в различных типах

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		высокопроизводительных систем **Уметь:** осуществлять контроль и мониторинг безопасности информации, расследование инцидентов информационной безопасности, тестирование и анализ защищенности информационных систем, администрирование систем защиты информации; уметь работать с различными инструментами разработки и использования программно-аппаратных средств защиты информации **Владеть:** Навыками контроля и мониторинга безопасности информации в высокопроизводительных системах Навыками тестирования и анализа защищенности высокопроизводительных систем Навыками администрирования систем защиты информации в высокопроизводительных систем

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	10 семестр	всего

Вид работы	Трудоемкость, академических часов	
	10 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**60,25**	**60,25**
Лекции (Л)	30	30
Лабораторные работы (ЛР)	30	30
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- написание реферата (Р);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);* *- изучение разделов электронного курса «Защита информации в высокопроизводительных системах» в системе обучения;* *- подготовка к лабораторным занятиям;* *- выполнение задания творческого уровня;* *- подготовка к зачету.*	**47,75**	**47,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 10 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Архитектурные основы высокопроизводительных систем и угрозы безопасности	38	10		10	18
2	Программно-аппаратные средства защиты HPC	35	10		10	15
3	Защита программного обеспечения в HPC	35	10		10	15
	Итого:	108	30		30	48
	Всего:	108	30		30	48

4.2 Содержание разделов дисциплины

РАЗДЕЛ 1. Архитектурные основы высокопроизводительных систем и угрозы безопасности

Введение в высокопроизводительные вычислительные системы. Определение высокопроизводительной системы (HPC) и её отличия от традиционных автоматизированных систем. Классификация HPC-систем: массово-параллельные (MPP), кластерные, векторно-конвейерные, гибридные. Основные компоненты компьютерного центра (КЦ): вычислительные узлы, коммуникационная сеть, управляющий сервер, система хранения данных (СХД). Принципы организации параллельных вычислений: MPI, OpenMP, CUDA. Показатели производительности HPC: пиковая и реальная производительность, масштабируемость. Эталонные тесты производительности. Требования ФСТЭК России к защите информации.

Модели угроз и нарушитель в HPC-системах. Понятие модели угроз для высокопроизводительной системы согласно ГОСТ Р 56546-2015. Типы нарушителей в HPC: внешний, внутренний (пользователь вычислительного узла), администратор. Основные каналы атак: через планировщик задач, через систему хранения данных, через коммуникационную сеть. Угрозы целостности вычислений (подмена результатов, модификация кода). Угрозы конфиденциальности (перехват данных между узлами, утечка через кэш-память). Угрозы доступности (DoS на коммутационную сеть, атаки на планировщик). Атаки на виртуализацию в HPC и контейнеризацию. Примеры реальных инцидентов в компьютерных центрах. Документирование модели угроз.

Организация параллельных вычислений и уязвимости. Принципы работы MPI: коммуникаторы, точки-точка, коллективные операции. Принципы работы OpenMP: разделение памяти, директивы компилятора, параллельные регионы. Уязвимости MPI-коммуникаций: перехват сообщений, подмена ранга, повтор, DoS. Атаки на коллективные операции MPI. Уязвимости OpenMP: гонки данных, утечки через кэш-память, несанкционированный доступ к общей памяти. Проблема доверия между MPI-процессами на разных узлах. Стандарты безопасности для MPI. Влияние защиты MPI на производительность.

Безопасность систем хранения данных в HPC. Архитектуры HPC-хранилищ. Угрозы для распределённых файловых систем в HPC: перехват данных, повреждение метаданных, DoS. Шифрование данных на диске и его влияние на производительность. Шифрование каналов доступа к хранилищу. Контроль целостности данных в распределённых файловых системах (мерклевы деревья, контрольные суммы). Разграничение доступа к данным в HPC-хранилищах. Аудит доступа к файлам и метаданным в HPC-среде. Изоляция пользовательских данных в общем хранилище.

Планировщики задач и управление доступом в HPC. Понятие планировщика задач в HPC. Популярные планировщики: SLURM, PBS/Torque, LSF, Grid Engine. Архитектура SLURM: контроллер, база данных, вычислительные узлы, демоны. Угрозы для планировщика задач: несанкционированный запуск задач, подмена приоритета, DoS. Аутентификация и авторизация в SLURM (MUNGE, LDAP, PAM). Изоляция пользовательских задач: контейнеризация (Singularity, Docker), виртуализация. Управление ресурсами и контроль использования: ограничения на CPU, память, время. Аудит действий планировщика. Методы защиты планировщика в соответствии с требованиями ФСТЭК.

РАЗДЕЛ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ HPC

Криптографическая защита в HPC: шифрование данных и коммуникаций. Роль криптографии в защите высокопроизводительных систем. Шифрование данных на диске в HPC. Шифрование коммуникаций между узлами. Специфика шифрования MPI-трафика. Аппаратные криптоускорители. Управление ключами в HPC-среде: генерация, распределение, хранение, ротация. Шифрование на уровне приложений в HPC. Проблема производительности: выбор алгоритмов шифрования для HPC. Требования ФСТЭК к криптографическим средствам защиты информации. Оценка накладных расходов при шифровании трафика.

Аппаратная изоляция в HPC. Понятие доверенных вычислительных сред (TEE) в HPC. Архитектура Intel Software Guard Extensions (SGX). Архитектура AMD Secure Encrypted Virtualization (SEV): шифрование памяти виртуальных машин. Применение SGX в HPC: защита отдельных вычислений от администратора и соседних процессов.

Защита от атак по побочным каналам в HPC. Понятие побочных каналов утечки информации. Классификация побочных каналов: кэш-атаки, атаки по времени, атаки по энергопотреблению, акустические атаки. Атаки на кэш-память в HPC-среде. Угроза для HPC: злоумышленник на соседнем ядре/узле может восстановить ключи шифрования или данные. Методы защиты от кэш-атак: изоляция кэша, обнуление кэша при переключении контекста. Атаки по времени в MPI-коммуникациях. Атаки по энергопотреблению в HPC. Пример уязвимости CVE-2017-9526 — раскрытие ключа EdDSA через наблюдение за побочными каналами. Методы противодействия: рандомизация времени выполнения, шумовые операции. Оценка защищённости HPC-системы от побочных каналов.

Системы обнаружения вторжений для HPC. Особенности применения IDS/IPS в высокопроизводительных системах. Сетевые IDS для HPC. Специфика сбора событий в HPC: масштабируемость, производительность, централизация. Интеграция IDS с планировщиком задач. Проблема ложных срабатываний в HPC-среде. Оценка влияния IDS на производительность вычислений. Автоматическое реагирование на инциденты в HPC.

Зонирование и сегментация сети в HPC-кластере. Понятие зон безопасности в суперкомпьютерном центре согласно требованиям ФСТЭК. Классификация зон: открытая сеть, управляющая сеть, вычислительная сеть, сеть хранения данных. Разделение информационно-вычислительной инфраструктуры на зоны безопасности. Межсетевые экраны для HPC: фильтрация на границах зон. Изоляция вычислительных узлов: отсутствие прямого доступа из внешней сети. Безопасность управляющей сети. Использование VLAN и VXLAN для сегментации HPC-сети. Мониторинг межзонового трафика. Пример архитектуры защищённого СКЦ с выделенными зонами. Оценка влияния сегментации на производительность коммуникаций.

РАЗДЕЛ 3. ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В HPC

Безопасная разработка HPC-приложений. Особенности разработки защищённого ПО для высокопроизводительных систем. Жизненный цикл разработки HPC-приложений с учётом безопасности. Типовые уязвимости в HPC-коде: переполнение буфера в MPI-буферах, гонки данных в OpenMP. Принципы безопасного программирования для HPC: валидация входных данных, минимизация привилегий. Статический анализ кода HPC-приложений: специфические правила для MPI/OpenMP. Динамический анализ: обнаружение гонок данных, проверка корректности MPI-коммуникаций. Требования к контролю отсутствия недекларированных возможностей (НДВ) согласно РД ФСТЭК. Безопасное управление памятью в HPC-приложениях. Примеры безопасных шаблонов проектирования для HPC. Инструменты анализа защищённости HPC-кода.

Тестирование безопасности HPC-систем. Виды тестирования безопасности для HPC: сканирование уязвимостей, пентест, аудит кода. Особенности пентеста суперкомпьютерных центров: ограничения по времени, влияние на производительность. Инструменты для сканирования уязвимостей HPC-инфраструктуры. Тестирование на проникновение в HPC-среду: этапы, методологии. Тестирование защищённости планировщика задач. Тестирование защищённости MPI-коммуникаций. Составление отчёта о тестировании безопасности HPC. Управление найденными уязвимостями (риск-ориентированный подход). Регрессионное тестирование после исправления уязвимостей. Юридические ограничения при тестировании СКЦ.

Мониторинг безопасности и управление инцидентами в HPC. Понятие мониторинга безопасности в реальном времени для HPC. Системы сбора и корреляции событий (SIEM) для суперкомпьютерных центров. Источники событий в HPC: логи SLURM, системные логи, сетевые устройства, IDS. Специфика сбора событий в HPC: объём данных, производительность. Настройка оповещений о подозрительной активности в HPC. Понятие инцидента информационной безопасности в КЦ. Этапы реагирования на инцидент в HPC-среде: сдерживание, устранение, восстановление. Автоматическое реагирование: блокировка пользователя, приостановка задач. Интеграция SIEM с планировщиком задач. Примеры SIEM-решений для HPC.

Контейнеризация и безопасность в HPC. Роль контейнеризации в HPC: изоляция пользовательских приложений, воспроизводимость. Популярные решения: Docker, Singularity/Apptainer, Shifter, Charliecloud. Особенности Singularity в HPC: поддержка непривилегированных контейнеров, интеграция с MPI. Угрозы безопасности при использовании контейнеров в HPC: эскалация привилегий, утечки данных. Безопасная сборка образов контейнеров для HPC. Управление образами: реестры, верификация подписей. Изоляция между контейнерами на одном узле. Интеграция контейнеров с планировщиком задач. Мониторинг безопасности контейнеров.

Аттестация и сертификация HPC-систем. Понятие аттестации HPC-системы на соответствие требованиям безопасности информации. Нормативные документы по аттестации (приказы ФСТЭК России). Классификация автоматизированных систем по требованиям защиты информации. Требования к межсетевым экранам для защиты HPC-сетей. Уровни контроля отсутствия недекларированных возможностей для ПО СЗИ. Требования к средствам антивирусной защиты для HPC-систем. Требования к защите от несанкционированного доступа (НСД). Порядок аттестации объекта информатизации. Эксплуатационная документация для аттестованной HPC-системы. Ответственность за эксплуатацию неаттестованных систем.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Исследование архитектуры высокопроизводительной системы	2
2	1	Разработка модели угроз для высокопроизводительной системы	2
3	1	Анализ уязвимостей MPI-приложений	2
4	1	Настройка защиты распределённого хранилища	2
5	1	Настройка безопасности планировщика SLURM	2
6	2	Реализация шифрования каналов связи в MPI-приложении	2
7	2	Разработка защищённого HPC-приложения с использованием	2

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
		Intel SGX	
8	2	Моделирование кэш-атаки в многопользовательской HPC-среде	2
9	2	Настройка системы обнаружения вторжений для HPC-кластера	2
10	2	Построение сегментированной сети для HPC-кластера	2
11	3	Статический анализ безопасности HPC-приложения	2
12	3	Проведение сканирования уязвимостей HPC-кластера	2
13	3	Развёртывание системы мониторинга безопасности для HPC-кластера	2
14	3	Настройка защищённых контейнеров для HPC-приложений	2
15	3	Разработка пакета документов для аттестации HPC-системы	2
		Итого:	30

5.1 Основная литература

1. Основы высокопроизводительных вычислений : учебное пособие / К. Е. Афанасьев, С. Ю. Завозкин, С. Н. Трофимов, А. Ю. Власенко. — Кемерово : КемГУ, [б. г.]. — Том 1 : Высокопроизводительные вычислительные системы — 2011. — 228 с. — ISBN 978-5-8353-1098-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/30123 (дата обращения: 09.04.2026). — Режим доступа: для авториз. пользователей.

2. Системы хранения данных : учебное пособие / Д. В. Гадасин, Д. Д. Рахмани, В. В. Маклачкова [и др.]. — Москва : МТУСИ, 2022. — 150 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/333794 (дата обращения: 20.02.2026). — Режим доступа: для авториз. пользователей.

5.2 Дополнительная литература

1. Рылов, С. А. Промышленный интернет. Современный подход и концепции : учебник / С. А. Рылов. — Москва : РТУ МИРЭА, 2023. — 124 с. — ISBN 978-5-7339-1969-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/386144 (дата обращения: 20.02.2026). — Режим доступа: для авториз. пользователей.

2. Импортозамещающие технологии обеспечения информационной безопасности и защиты данных : учебное пособие / Д. А. Короченцев, Л. В. Черкесова, Е. А. Ревякина [и др.]. — Ростов-на-Дону : Донской ГТУ, 2021. — 335 с. — ISBN 978-5-7890-1893-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237782 (дата обращения: 20.02.2026). — Режим доступа: для авториз. пользователей.

3. Бобков, С. Г. Высокопроизводительные системы и подсистемы памяти : учебное пособие / С. Г. Бобков. — Москва : НИЯУ МИФИ, 2018. — 48 с. — ISBN 978-5-7262-2514-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126651 (дата обращения: 09.04.2026). — Режим доступа: для авториз. пользователей.

5.3 Периодические издания

1. Закон и право - https://eivis.ru/browse/publication/81027/udb/12/ закон-и-право
2. Защита информации. Инсайд - https://eivis.ru/browse/publication/122426/udb/12/ защита-информации-инсайд

5.4 Интернет-ресурсы

1. Безопасность IIS: Информация. – Режим доступа: https://intuit.ru/studies/courses/1002/122/info

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система РЕД ОС.
2. Пакет офисных приложений «МойОфис Образование»
3. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..
4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ http://garant.net.osu.ru
5. Автоматизированная интерактивная система сетевого тестирования - АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа - http://aist.osu.ru.
6. OWASP https://owasp.org/www-project-top-ten//
7. CVE https://cve.mitre.org//
8. Common Attack Pattern Enumeration and Classification (CAPEC) https://capec.mitre.org/.
9. Банк данных угроз безопасности информации https://bdu.fstec.ru/vul.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, курсового проектирования, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный персональными компьютерами с установленным программным обеспечением.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.