

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 09:20:01

Уникальный программный ключ

fd935d10451b860e912264c0378f8448452b693f94388008e29877a6bcbf5

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»**

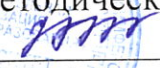
«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»

Факультет экономики, управления и юриспруденции

Кафедра «Управление и бизнес-информатика»

УТВЕРЖДАЮ

Проректор по учебно-методической работе

 / Г.П. Узунова

«02» февраля 2026 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность Astra Linux

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

Симферополь, 2026

Рабочая программа составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность» профиль Безопасность компьютерных систем, утвержденным приказом Министерства образования и науки Российской Федерации от 17.11.2020 г. № 1427 (зарегистрировано в Министерстве юстиции РФ 18.02.2021 №62548) с изменениями и дополнениями.

Программу составил Фурин А.Д. преподаватель

Рабочая программа дисциплины «Безопасность Astra Linux» утверждена на заседании кафедры «Управление и бизнес-информатика».

Протокол № 6 от 29.01.2026 г.

Заведующий кафедрой  Д.В. Моторина
(подпись)

АННОТАЦИЯ	
Индекс дисциплины по учебному плану	Наименование дисциплины
Б1.В.05	Безопасность Astra Linux
Цель изучения дисциплины	формирование у студентов профессиональных компетенций, необходимых для установки, настройки и администрирования защищенной операционной системы специального назначения (Astra Linux Special Edition) в соответствии с требованиями российских регуляторов.
Место дисциплины в структуре ОПОП	Дисциплина Основы информационной безопасности относится к базовой части ОПОП и является обязательной для освоения.
Компетенции, формируемые в результате освоения дисциплины	ПК-2
Содержание дисциплины	Тема 1. Архитектура уровней защищенности Astra Linux: «Орёл», «Воронеж», «Смоленск». Тема 2. Мандатная модель разграничения доступа (МРД): метки конфиденциальности и неиерархические категории. Тема 3. Мандатный контроль целостности (МКЦ) и замкнутая программная среда (ЗПС). Тема 4. Подсистема аудита и регистрация событий безопасности. Тема 5. Управление пользователями, ролями и парольные политики в среде МАС. Тема 6. Средства защиты виртуализации и контейнеризации в экосистеме Astra Linux
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)
Форма промежуточной аттестации	Зачет

Содержание

1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата	5
2. Место дисциплины в структуре ОПОП бакалавриата	5
3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся	5
4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	6
5. Контроль качества освоения дисциплины	11
6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	11
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	12
8. Методические указания для обучающихся по освоению дисциплины	13
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)	13
10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине	14

1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата

Цель изучения дисциплины «Безопасность Astra Linux» – формирование у студентов профессиональных компетенций, необходимых для установки, настройки и администрирования защищенной операционной системы специального назначения (Astra Linux Special Edition) в соответствии с требованиями российских регуляторов.

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-2	Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации потребностей личности, общества и государства	ПК-2.1. Знает организацию работы и нормативные правовые акты по аттестации объектов информатизации, методы аттестации уровня защищенности информационных систем; ПК-2.2. Умеет участвовать в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации. ПК-2.3 владеет методиками проверки защищенности объектов информатизации на соответствие нормативных документов

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Безопасность Astra Linux относится к базовой части ОПОП и является обязательной для освоения, изучается обучающимися очной формы обучения в 5 семестре, очно-заочной формы обучения – в 5 семестре.

Дисциплина является базовой для освоения курсов дисциплин профессиональной подготовки.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единицы (з.е.), 108 академических часа.

3.1. Объём дисциплины по видам учебных занятий (в часах)

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 3 зачётных единицы 108 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	108
Контактная работа	38

Аудиторная работа (всего):	38
Лекции	12
Семинары, практические занятия	26
Самостоятельная работа обучающихся (всего)	70
Зачет	+

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 3 зачётных единицы 108 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	108
Контактная работа	28
Аудиторная работа (всего):	28
Лекции	10
Семинары, практические занятия	18
Самостоятельная работа обучающихся (всего)	80
Зачет	+

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоёмкость по видам учебных занятий (в академических часах)

№ темы	Наименование темы	Всего		Количество часов					
		ОФО	ОЗФО	Контактная работа				Внеаудит. работа	
				Лекции		Практические		Самост. работа	
				ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО
1.	Тема 1. Архитектура уровней защищенности Astra Linux: «Орёл», «Воронеж», «Смоленск».	18	18	2	2	4	2	12	12
2.	Тема 2. Мандатная модель разграничения доступа (МРД): метки конфиденциальности и неиерархические категории.	18	18	2	2	4	4	12	12
3.	Тема 3. Мандатный контроль целостности (МКЦ) и замкнутая программная среда (ЗПС).	18	18	2	2	4	4	12	14
4.	Тема 4. Подсистема аудита и регистрация событий безопасности.	18	18	2	1	4	4	12	14
5.	Тема 5. Управление пользователями, ролями и парольные политики в среде	18	18	2	1	4	2	12	14

	MAC.								
6.	Тема 6. Средства защиты виртуализации и контейнеризации в экосистеме Astra Linux	18	18	2	2	6	2	10	14
	Всего по дисциплине	108	108	12	10	26	18	70	80
	Контроль	-	-						
	Итого	108	108						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Архитектура уровней защищенности Astra Linux: «Орёл», «Воронеж», «Смоленск» Раскрывается концепция сертифицируемых версий ОС. Изучаются различия между базовым, усиленным и максимальным уровнями защиты. Рассматривается соответствие каждого уровня требованиям ФСТЭК (классы защиты АС), ФСБ и Минобороны РФ. Анализируется состав доступных средств защиты в зависимости от выбранного режима функционирования системы при установке.

Тема 2. Мандатная модель разграничения доступа (МРД): метки конфиденциальности и неиерархические категории Детально рассматривается механизм принудительного управления доступом MAC (*Mandatory Access Control*). Изучается структура меток безопасности субъектов (пользователей/процессов) и объектов (файлов/устройств): уровни секретности (от «несекретно» до особой важности») и наборы неиерархических категорий. Раскрываются правила доминирования меток и логика работы ядра PARSEC при проверке прав доступа к файлам.

Тема 3. Мандатный контроль целостности (МКЦ) и замкнутая программная среда (ЗПС) Рассматриваются механизмы защиты самой операционной системы от модификации. МКЦ предотвращает несанкционированную запись в системные файлы даже пользователем с высокими привилегиями. Изучается ЗПС: использование электронной подписи исполняемых файлов и скриптов, проверка целостности перед запуском и блокировка выполнения недоверенного кода, что исключает запуск вредоносного ПО без ведома администратора.

Тема 4. Подсистема аудита и регистрация событий безопасности Изучается архитектура ведения журналов в защищенном режиме. Рассматриваются возможности детальной фиксации событий: вход/выход из системы, обращение к объектам по МРД, изменение полномочий, попытки нарушения целостности. Особое внимание уделяется настройке удаленной передачи логов на выделенный сервер сбора данных и защите самого хранилища журналов от удаления или подмены злоумышленником.

Тема 5. Управление пользователями, ролями и парольные политики в среде MAC Анализируются особенности создания учетных записей в контексте мандатного доступа. Изучается механизм ролей (администратор системы, офицер безопасности, пользователь), разделение административных обязанностей. Рассматриваются инструменты централизованного управления политиками сложности паролей, срока их действия, а также ограничения сессий по времени и привязка пользователей к конкретным терминалам.

Тема 6. Средства защиты виртуализации и контейнеризации в экосистеме Astra Linux Раскрываются методы безопасного развертывания гостевых операционных систем и изолированных приложений. Изучается работа гипервизора (KVM) с наследованием меток безопасности (каждая ВМ получает свой контекст МРД). Рассматриваются механизмы изоляции контейнеров (*Docker/LXC*) средствами мандатного

контроля, предотвращающие утечку данных между контейнерами и обеспечивающие безопасность платформы оркестрации (*Kubernetes*) на базе отечественной ОС

4.3. Содержание практических занятий (очная форма обучения)

Разделы, темы, дидактические единицы
Тема 1. Архитектура уровней защищенности Astra Linux: «Орёл», «Воронеж», «Смоленск» Раскрывается концепция сертифицируемых версий ОС. Изучаются различия между базовым, усиленным и максимальным уровнями защиты. Рассматривается соответствие каждого уровня требованиям ФСТЭК (классы защиты АС), ФСБ и Минобороны РФ.
Тема 2. Мандатная модель разграничения доступа (МРД): метки конфиденциальности и неиерархические категории Детально рассматривается механизм принудительного управления доступом MAC (<i>Mandatory Access Control</i>). Изучается структура меток безопасности субъектов (пользователей/процессов) и объектов (файлов/устройств): уровни секретности (от «несекретно» до особой важности») и наборы неиерархических категорий.
Тема 3. Мандатный контроль целостности (МКЦ) и замкнутая программная среда (ЗПС) Рассматриваются механизмы защиты самой операционной системы от модификации. МКЦ предотвращает несанкционированную запись в системные файлы даже пользователем с высокими привилегиями.
Тема 4. Подсистема аудита и регистрация событий безопасности Изучается архитектура ведения журналов в защищенном режиме. Рассматриваются возможности детальной фиксации событий: вход/выход из системы, обращение к объектам по МРД, изменение полномочий, попытки нарушения целостности.
Тема 5. Управление пользователями, ролями и парольные политики в среде MAC Анализируются особенности создания учетных записей в контексте мандатного доступа. Изучается механизм ролей (администратор системы, офицер безопасности, пользователь), разделение административных обязанностей.
Тема 6. Средства защиты виртуализации и контейнеризации в экосистеме Astra Linux Раскрываются методы безопасного развертывания гостевых операционных систем и изолированных приложений. Изучается работа гипервизора (<i>KVM</i>) с наследованием меток безопасности (каждая ВМ получает свой контекст МРД).

4.4. Содержание самостоятельной работы

Разделы, темы, дидактические единицы
Тема 1. Архитектура уровней защищенности Astra Linux: «Орёл», «Воронеж», «Смоленск» Состав доступных средств защиты в зависимости от выбранного режима функционирования системы при установке.
Тема 2. Мандатная модель разграничения доступа (МРД): метки конфиденциальности и неиерархические категории Правила доминирования меток и логика работы ядра <i>PARSEC</i> при проверке прав доступа к файлам.
Тема 3. Мандатный контроль целостности (МКЦ) и замкнутая программная среда (ЗПС) ЗПС: использование электронной подписи исполняемых файлов и скриптов, проверка целостности перед запуском и блокировка выполнения недоверенного кода, что исключает запуск вредоносного ПО без ведома администратора.

Тема 4. Подсистема аудита и регистрация событий безопасности Настройка удаленной передачи логов на выделенный сервер сбора данных и защите самого хранилища журналов от удаления или подмены злоумышленником.
Тема 5. Управление пользователями, ролями и паролями политики в среде МАС Инструменты централизованного управления политиками сложности паролей, срока их действия, а также ограничения сессий по времени и привязка пользователей к конкретным терминалам.
Тема 6. Средства защиты виртуализации и контейнеризации в экосистеме Astra Linux Механизмы изоляции контейнеров (<i>Docker/LXC</i>) средствами мандатного контроля, предотвращающие утечку данных между контейнерами и обеспечивающие безопасность платформы оркестрации (<i>Kubernetes</i>) на базе отечественной ОС

5. Контроль качества освоения дисциплины

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся в Автономной некоммерческой организации «Образовательная организация высшего образования» «Университет экономики и управления».

Вид промежуточной аттестации – зачет. Форма проведения промежуточной аттестации – письменный зачет.

Фонд оценочных средств по дисциплине приведен в приложении к РПД.

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература:

1. Батуро, А. Н. Прикладное программное обеспечение под ОС Astra Linux Special Edition : учебное пособие / А. Н. Батуро, Г. М. Бойко. — Железнодорожск : Сибирская пожарно-спасательная академия ГПС МЧС России, 2025. — 346 с. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/149782/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

2. Фомин, Д. В. Информационная безопасность : учебник / Д. В. Фомин. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/118876.html> (дата обращения: 03.07.2025). — Режим доступа: для авторизир. пользователей

б) дополнительная литература:

3. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 с. — ISBN 978-5-4487-1026-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/142805.html> (дата обращения: 20.03.2025). — Режим доступа: для авторизир. пользователей

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

1. Информационно-правовой портал «Гарант»: официальный сайт. — URL: <http://www.garant.ru> — Текст: электронный.

2. Цифровой образовательный ресурс «IPRsmart»: официальный сайт. – URL: <http://www.iprbookshop.ru/> – Текст: электронный.

3. Научная электронная библиотека «КиберЛенинка»: официальный сайт. – URL: <https://cyberleninka.ru/> – Текст: электронный.

4. Российский интернет-портал и аналитическое агентство TAdviser: официальный сайт. – URL: <https://www.tadviser.ru/> – Текст: электронный.

8. Методические указания для обучающихся по освоению дисциплины

При проведении лекций, семинарских (практических) занятий, самостоятельной работе обучающихся применяются интерактивные формы проведения занятий с целью погружения обучающихся в реальную атмосферу профессионального сотрудничества по разрешению проблем, оптимальной выработки навыков и качеств будущего специалиста. Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и обучающиеся) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуацию.

В учебном процессе используются интерактивные формы занятий:

- творческое задание. Выполнение творческих заданий требует от обучающегося воспроизведение полученной ранее информации в форме, определяемой преподавателем, и требующей творческого подхода;

- групповое обсуждение. Групповое обсуждение кого-либо вопроса направлено на достижение лучшего взаимопонимания и способствует лучшему усвоению изучаемого материала.

В ходе освоения дисциплины при проведении контактных занятий используются следующие формы обучения, способствующие формированию компетенций: лекции-дискуссии; кейс-метод; решение задач; ситуационный анализ; обсуждение рефератов и докладов; разработка групповых проектов; встречи с представителями государственных и общественных организаций.

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

В процессе лекционных и практических занятий используется следующее программное обеспечение:

- *программы, обеспечивающие доступ в сеть «Интернет» (например, «Microsoft Edge», «Google Chrome»);

- *программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);

- *текстовые редакторы и процессоры (например, «Microsoft Office Word»);

- *табличные процессоры (например, «Microsoft Office Excel»);

- *системы управления базами данных (например, «Microsoft Office Access»);

- *программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»);

- *проблемно-ориентированные пакеты прикладных программ по отраслям и сферам деятельности (например, «1С: Управление нашей фирмой», «Loginom Community Edition»).

10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине

Учебная аудитория

Оборудование учебного кабинета:

- рабочее место преподавателя;
- посадочные места по количеству обучающихся;
- доска классная;
- стенды информационные.

Учебно-наглядные пособия:

- ноутбук с лицензионным программным обеспечением и возможностью подключения к информационно-телекоммуникационной сети Интернет;
- мультимедийная установка.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.