

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 08:54:43

Уникальный программный ключ:

fd935d10451b860e912264c0378f8448453b5fdb607f94788008e29877e6bcb55

**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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Безопасность Astra Linux

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

Симферополь, 2026

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Средства оценивания в ходе текущего контроля:

- устные опросы в ходе семинарских занятий;
- рефераты;
- тестирование;
- практические и ситуационные задания, выполняемые в ходе семинарского занятия или рекомендуемые для самостоятельной работы.

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

1.1. Вопросы к текущему контролю

1. Сравнение архитектуры подсистемы безопасности ОС Windows и Astra Linux Special Edition.
2. Мандатная сущностно-ролевая ДП-модель управления доступом: основные понятия (субъект, объект, сущность, метка безопасности).
3. Иерархия уровней конфиденциальности в Astra Linux (от «не определено» до особой важности) и их числовые значения.
4. Неиерархические категории секретности: назначение, создание и применение для реализации принципа минимальных привилегий.
5. Правила доминирования меток безопасности субъектов и объектов. Условия предоставления доступа при чтении и записи.
6. Механизм наследования меток безопасности при создании новых файлов и каталогов.
7. Особенности работы с объектами нулевой метки (несекретными данными) в сессии пользователя с ненулевым уровнем допуска.
8. Влияние МКЦД на работу стандартных утилит администрирования (*sudo*, *su*) и межпроцессное взаимодействие.
9. Понятие «сущность» в модели PARSEC и её отличие от традиционного объекта файловой системы.
10. Назначение подсистемы принудительного контроля доступа PARSEC. Составные части модуля (база защиты, ядро, библиотеки).
11. Мандатный контроль целостности (МКЦ): уровни целостности, правила взаимодействия процессов разного уровня целостности.
12. Механизм замораживания процесса (*freeze*): причины срабатывания, влияние на пользовательскую сессию, способы диагностики и снятия блокировки.

13. Роль службы *parsec* и демона *astra-mount*. Порядок загрузки модулей безопасности.
14. Управление списками ПРД (правил разграничения доступа) через графический интерфейс и утилиты командной строки (*pdpl*, *pdp-id*).
15. Механизм очистки памяти и гарантированного уничтожения информации при удалении объектов.
16. Замкнутая программная среда (ЗПС): механизм электронной подписи исполняемых файлов (*gostsum*, *.sig* файлы).
17. Последствия нарушения целостности исполняемого файла или его цифровой подписи. Работа механизма АРТ при включенной ЗПС.
18. Пространства имен (*namespaces*) и изоляция ресурсов в Astra Linux: практическое применение контейнеризации без стороннего ПО.
19. Модель Privileged User Identity (PUI): отказ от прямого использования учетной записи *root*, механизмы повышения привилегий (*fly-admin-smc*, *sudo*).
20. Безопасная работа со сменными носителями: автоматическая маркировка согласно уровню сессии, запрет копирования данных вверх/вниз.
21. Механизм сокетов фильтрации (*seccomp*) и ограничения системных вызовов для изолированных приложений.
22. Интеграция с КриптоПро CSP/CAAdES: установка пакетов, проверка работоспособности, типичные ошибки при подписании документов.
23. Функциональные роли СКЗИ в составе ОС: защищенный канал связи (VPN), шифрование дисков (LUKS + ГОСТ), электронная подпись.
24. Работа с ключевыми контейнерами и сертификатами X.509 в среде Astra Linux. Отличие хранения ключей в реестре, файле и на токене.
25. Настройка защищенного удаленного доступа (VDI/VNC/RDP) с использованием встроенных средств ГОСТ-шифрования.
26. Подсистема аудита безопасности: формат записей в журнале, ключевые события (изменение меток, попытки НСД, запуск непривилегированных процессов).
27. Централизованный сбор логов (*auditd*, *syslog-ng*). Настройка пересылки событий на сервер сбора событий безопасности.
28. Автоматизированный анализ журналов безопасности (AIDE, встроенные отчеты *fly-admin-report*). Выявление аномалий поведения пользователей.
29. Режимы работы ядра безопасности: различия между максимальным, базовым и штатным режимами функционирования (и их влияние на производительность).
30. Комплексный сценарий: настройка безопасной многопользовательской среды, где пользователи разных отделов (грифы «Секретно» и «Для служебного пользования») работают на одной рабочей станции одновременно, не имея возможности обмениваться файлами и буфером обмена.

1.2. Темы рефератов

1. Сравнительный анализ мандатных моделей управления доступом: Белла — Лападулы, Биба и сущностно-ролевой ДП-модели в Astra Linux Special Edition.
2. Эволюция подсистемы PARSEC от ранних версий (Astra Linux 1.4/1.5) до архитектуры версии 1.8: изменения в механизме меток и производительности ядра.
3. Мандатный контроль целостности (МКЦ) как средство защиты от атак типа *rootkit* и несанкционированной модификации системных библиотек.
4. Концепция Privileged User Identity (PUI): архитектурные преимущества отказа от прямого использования учетной записи *root* для минимизации поверхности атаки.
5. Механизм гарантированного уничтожения информации при удалении объектов в файловых системах EXT4/Btrfs под управлением МКЦД.

6. Практическая реализация иерархических уровней конфиденциальности и неиерархических категорий секретности на примере многопользовательской системы документооборота.

7. Проблема скрытых каналов передачи информации в ОС с мандатным контролем доступа и методы их перекрытия в архитектуре Astra Linux.

8. Автоматизация маркировки документов: интеграция Astra Linux со средствами оптического распознавания текста (OCR) и принудительного проставления меток PDF-файлов.

9. Особенности реализации правил взаимодействия процессов разного уровня целостности (заморозка процесса, передача данных через буфер обмена).

10. Управление жизненным циклом прав доступа: делегирование полномочий администраторам безопасности без нарушения принципа наименьших привилегий.

11. Замкнутая программная среда (ЗПС) на базе электронной подписи: влияние на процесс разработки прикладного ПО и администрирования серверов.

12. Механизмы обеспечения доверенной загрузки (UEFI Secure Boot) и контроля целостности программной среды до старта ядра Linux (взаимодействие с ПАК СЗИ «Соболь» или ViPNet SafeBoot).

3. Проблемы совместимости современного контейнеризованного ПО (*Docker*, *Podman*) с механизмами ЗПС и пути их решения в инфраструктуре заказчика.

14. Анализ отказоустойчивости ЗПС: сценарии работы операционной системы при компрометации базы подписей исполняемых файлов.

15. Интеграция сертифицированных СКЗИ (например, КриптоПро CSP) с системными службами аутентификации (PAM) и печати (CUPS-GOST).

16. Организация защищенного удаленного доступа к графическим сессиям VDI/VNC с использованием отечественных алгоритмов шифрования ГОСТ.

17. Безопасное хранение закрытых ключей пользователей: сравнительный анализ программных токенов, реестра Windows (через Wine/Crostini) и аппаратных носителей (Рутокен, JaCarta).

18. Применение криптопровайдеров класса HSM (Hardware Security Module) для централизованной проверки электронных подписей в высоконагруженных сервисах на базе Astra Linux.

19. Проектирование системы централизованного сбора и корреляции событий безопасности Astra Linux (на базе стека ELK/Elasticsearch, Logstash, Kibana или MaxPatrol SIEM).

20. Методика расследования инцидентов ИБ в среде Astra Linux SE: разбор кейса несанкционированного повышения привилегий через механизмы межпроцессного взаимодействия (IPC) и пространства имен.

1.3. Тестовые задания

0. **1. Какой механизм является основным для реализации мандатного контроля доступа (МКЦД) в Astra Linux Special Edition?** а) SELinux б) AppArmor в) Подсистема PARSEC г) Стандартные права *chmod/rwx* **Правильный ответ: в**
1. **2. Что произойдет, если пользователь с уровнем допуска «Для служебного пользования» попытается прочитать файл с меткой «Секретно»?** а) Файл будет скопирован, но помечен как «Для служебного пользования» б) Доступ будет разрешен после ввода пароля администратора в) В доступе будет отказано из-за нарушения правил доминирования меток г) Уровень файла автоматически понизится до уровня пользователя **Правильный ответ: в**
2. **3. Какая утилита используется администратором для просмотра и управления метками безопасности файлов из командной строки?** а) `ls -l` б) `pdpl` в) `chmod` г) `stat` **Правильный ответ: б**

3. **4. За что отвечает механизм Замкнутой программной среды (ЗПС) в Astra Linux?** а) За шифрование всего жесткого диска б) За контроль целостности исполняемых файлов на основе их электронной подписи перед запуском в) За блокировку USB-портов г) За автоматическое обновление системы только из доверенных репозиториях
Правильный ответ: б
4. **5. Что такое уровень целостности в контексте МКЦ (мандатного контроля целостности)?** а) Скорость работы процессора при проверке подписей б) Степень доверия к источнику данных или процессу, защищающая системные файлы от модификации менее доверенными субъектами в) Версия установленного пакета обновлений безопасности г) Количество антивирусных баз, загруженных в память
Правильный ответ: б
5. **6. Если процесс пытается записать данные в файл с более высоким уровнем конфиденциальности, чем у самого процесса, сработает правило модели Белла — Лападулы:** а) «No read up» (нельзя читать вверх) б) «No write down» (нельзя писать вниз) в) «No write up» (нельзя писать вверх) г) «Simple integrity property»
Правильный ответ: в
6. **7. Какое действие необходимо выполнить сразу после установки Astra Linux SE для корректной работы механизмов ЗПС и МКЦД?** а) Установить драйверы видеокарты Nvidia б) Задать пароль пользователю root и включить его в группу sudo в) Сгенерировать локальные ключи защиты и инициализировать базу меток безопасности г) Отключить сетевой экран (ufw)
Правильный ответ: в
7. **8. Что означает состояние процесса «заморожен» (frozen) в графической сессии Astra Linux?** а) Процесс потребляет 100% ресурсов ЦП б) Процесс попытался нарушить правила мандатного контроля целостности (например, передать данные между разными уровнями через буфер обмена) в) У пользователя закончилась оперативная память г) Антивирус поместил процесс в карантин
Правильный ответ: б
8. **9. Где хранятся журналы аудита событий безопасности по умолчанию?** а) В каталоге /var/log/parsec/ б) В домашнем каталоге пользователя /home/user/ в) В корне файловой системы /audit/ г) Журналы не ведутся без установки КриптоПро
Правильный ответ: а
9. **10. Можно ли стандартными средствами ОС (через проводник Fly или команду ср) скопировать информацию из документа уровня «Секретно» в документ уровня «Несекретно»?** а) Да, если пользователь является владельцем обоих файлов б) Да, если отключить ЗПС перед копированием в) Нет, это запрещено механизмом предотвращения утечки информации («запись вниз») г) Да, если размер файла меньше 1 МБ
Правильный ответ: в
10. **11. Какую роль выполняет подсистема PUI (Privileged User Identity)?** а) Позволяет любому пользователю запускать команды от имени root без пароля б) Обеспечивает выполнение административных задач через делегирование привилегий без использования прямой учетной записи суперпользователя в) Автоматически меняет пароль root каждые 24 часа г) Скрывает процессы других пользователей в диспетчере задач
Правильный ответ: б
11. **12. Для чего предназначен комплекс средств защиты информации (КСЗИ) в составе дистрибутива?** а) Только для обеспечения совместимости с Windows-программами б) Для выполнения требований регуляторов (ФСТЭК России) по защите конфиденциальной информации и государственной тайны в) Исключительно для ускорения загрузки операционной системы г) Для автоматического создания резервных копий каждые 15 минут
Правильный ответ: б
12. **13. Что проверяет механизм ЗПС непосредственно перед выполнением бинарного файла?** а) Наличие свободного места на диске б) Соответствие хеш-суммы файла и наличие валидной электронной подписи разработчика в) IP-адрес компьютера, с которого запущен файл г) Имя текущего пользователя в системе
Правильный ответ: б

13. **14. При создании нового файла в папке с меткой «Уровень 2», какой меткой он будет обладать изначально?** а) Меткой «Не определено» б) Меткой родительского каталога («Уровень 2») согласно правилам наследования в) Самой низкой меткой в системе («Несекретно») г) Меткой запрашивается интерактивно у пользователя
Правильный ответ: б
14. **15. Какой протокол удаленного доступа рекомендуется использовать в защищенном контуре Astra Linux для передачи графического интерфейса с соблюдением требований по шифрованию?** а) HTTP б) Telnet в) SSH (с поддержкой ГОСТ-алгоритмов) или специализированный VDI/VNC со встроенным СКЗИ г) FTP
Правильный ответ: в
15. Дополнить: В операционной системе Astra Linux Special Edition мандатный контроль целостности (МКЦ) предназначен для защиты системных файлов от несанкционированной модификации субъектами с более низким уровнем _____.
(Ответ: целостности)
16. Дополнить: Для принудительного завершения «замороженного» (*frozen*) процесса, возникшего из-за нарушения правил МКЦ, администратор использует утилиту _____.
(Ответ: fly-unfreez / fly-admin-freeze)
17. Дополнить: В архитектуре PARSEC метка безопасности состоит из иерархического уровня конфиденциальности и набора неиерархических _____.
(Ответ: категорий)
18. Дополнить: Замкнутая программная среда (ЗПС) блокирует запуск исполняемого файла в случае отсутствия или нарушения его электронной _____.
(Ответ: подписи / ЭП)
19. Дополнить: Согласно модели Белла — Лападулы, реализованной в МКЦД, запрещено чтение данных вверх по иерархии уровней, что описывается правилом «No _____.
(Ответ: read)
20. Дополнить: При копировании файла в пределах одной директории наследование метки происходит от родительского _____.
(Ответ: каталога / контейнера)
21. Дополнить: Для централизованного сбора и анализа событий аудита безопасности из журналов /var/log/parsec/ используется протокол _____.
(Ответ: syslog / auditd)
22. Дополнить: Механизм Privileged User Identity (PUI) реализует принцип наименьших привилегий, исключая необходимость постоянной работы под учетной записью _____.
(Ответ: root / суперпользователя)
23. Дополнить: Для обеспечения доверенной загрузки ОС до старта ядра Linux в связке с Astra Linux SE применяются аппаратные модули, такие как ПАК СЗИ «_____».
(Ответ: Соболев)
24. Дополнить: В режиме сцепления блоков шифротекста (СБС) для зашифрования первого блока открытого текста используется вектор _____.
(Ответ: инициализации / IV)
25. Дополнить: Для управления мандатными атрибутами объектов и субъектов из командной строки предназначена базовая утилита _____.
(Ответ: pdpl)
26. Дополнить: При включенной ЗПС установка сторонних пакетов через менеджер АРТ возможна только при наличии цифровой _____ репозитория в локальном хранилище ключей.
(Ответ: подписи)
27. Дополнить: Мандатное управление доступом в Astra Linux реализует ДП-модель, которая является сущностно-ролевой моделью с контролем _____ потоков информации.
(Ответ: скрытых)
28. Дополнить: Для работы с российскими криптографическими алгоритмами (ГОСТ Р 34.10-2012) в подсистеме проверки подлинности (РАМ) интегрируется СКЗИ КристоПро _____.
(Ответ: CSP)
29. Дополнить: Очистка освобождаемых областей оперативной памяти и дисковых блоков в Astra Linux SE выполняется для предотвращения утечки остаточной _____.
(Ответ: информации)

1.4. Практические задания

1. Задача: Процесс проверки электронной подписи ГОСТ Р 34.10-2012 в КриптоПро CSP на рабочей станции занимает 15 миллисекунд. Рассчитайте максимальное количество документов, которые пользователь может подписать за одну рабочую смену (8 часов), если на подготовку документа уходит 10 секунд. *Ответ:* Время одной итерации = 10,015 сек. Всего секунд в смене = 28 800. Пропускная способность смены = $28\,800 / 10,015 \approx 2\,875$ документов.

2. Задача: Аппаратный токэн выполняет вычисление хеш-функции ГОСТ Р 34.11-2012 («Стрибог») для блока данных объемом 1 МБ за 20 миллисекунд. Какова максимальная скорость обработки потока данных этим устройством в мегабайтах в секунду? *Ответ:* $1 / 0,02 \text{ сек} = 50 \text{ МБ/сек.}$

3. Задача: Межсетевой экран на базе Astra Linux шифрует трафик со скоростью 900 Мбит/сек. При этом на каждый пакет накладывается задержка в 2 микросекунды из-за работы модуля ЗПС. Каков максимальный размер пакета (в байтах), при котором устройство еще способно поддерживать указанную скорость без накопления очереди? (Для упрощения считать, что 1 бит = 1 операция). *Ответ:* Скорость в операциях/сек = $900 * 10^6 / 8 = 112\,500\,000$ пакетов/сек. Размер = $1 / 112\,500\,000 / 0,000002 \text{ сек} \approx 444$ байта.

4. Задача: Система аудита генерирует 500 событий безопасности в секунду. Каждое событие занимает в среднем 256 байт. Хватит ли пропускной способности шины записи дискового массива 10 МБ/сек для предотвращения потери логов? *Ответ:* Поток данных = $500 * 256 = 128\,000$ байт/сек (0,122 МБ/сек). *Ответ:* Да, хватит с запасом.

5. Задача: В системе работают три пользователя с уровнями допуска: П1 — «Уровень 1», П2 — «Уровень 2», П3 — «Уровень 3». Файл А имеет метку «Уровень 2». Кто из пользователей сможет прочитать файл? Кто сможет его модифицировать (записать)? *Ответ:* Прочитать смогут П2 и П3 (правило No read up). Записать сможет только П1 (правило No write down; запись разрешена на свой уровень или выше, но модификация требует равенства уровней целостности/конфиденциальности в строгой ДП-модели, здесь подразумевается классическая модель Белла-Лападулы для чтения и обратная для записи вниз, однако в контексте модификации субъект должен доминировать над объектом, а объект не должен доминировать над субъектом для записи вверх. В классической задаче: читать $\leq$ свой уровень, писать $\geq$ свой уровень. Если следовать строго модели Б-Л: чтение P2, P3; запись P1, P2).

6. Задача: Пользователь создает новый текстовый файл в каталоге /opt/data, который помечен как {2, КВ, КТ} (Уровень 2, категории Бухгалтерия, Кадры). Какой будет начальная метка файла согласно правилам наследования, если у пользователя сессия {3, КВ}? *Ответ:* {2, КВ}. Уровень берется от родителя (директории), категория — пересечение категорий родителя и сессии (КВ).

7. Задача: Администратор пытается скопировать данные через буфер обмена из терминала с меткой «Секретно» в открытое окно браузера (метка «Несекретно»). Опишите состояние процессов после нажатия Ctrl+C в окне терминала. *Ответ:* Процесс терминала перейдет в состояние «заморожен» (frozen) из-за нарушения правила мандатного контроля целостности (попытка передачи данных вниз).

8. Задача: На сервере хранятся документы трех грифов: НС (Несекретно), С (Секретно), СС (Совершенно секретно). Стоимость утечки одного документа: НС — 0 руб., С — 1 млн руб., СС — 10 млн руб. Вероятность взлома сервера одинакова для всех зон. Где выгоднее разместить систему обнаружения вторжений (IDS) стоимостью 500 тыс. руб., чтобы минимизировать риск? *Ответ:* Над зоной «СС», так как ожидаемый ущерб (10 млн) значительно превышает стоимость защиты.

9. Задача: Объект имеет метку {1, КатА}. Субъекты имеют метки: S1:{1, КатА}, S2:{2, КатА}, S3:{1, КатБ}. Расположите субъектов в порядке возможности доступа к объекту для операции ЧТЕНИЯ. *Ответ:* S1 (полный доступ), S2 (доступ по уровню, если нет запрета по категориям), S3 (запрещено, категории не пересекаются).

10. Задача: Размер исполняемого файла nginx составляет 5 МБ. Скорость чтения диска — 500 МБ/сек, вычислительная мощность позволяет проверять подпись ГОСТ со скоростью 100 МБ/сек. Каково минимальное время запуска сервиса с включенной ЗПС? *Ответ:* Ограничение по проверке подписи: $5 / 100 = 0,05$ сек (50 мс).

11. Задача: При обновлении системы АРТ скачивает пакет размером 20 МБ. Скорость канала — 10 Мбит/сек. Вычислите, сколько времени займет только фаза проверки цепочки доверия GPG-подписи Release-файла, если проверка одного килобайта подписи занимает 0,5 мс. *Ответ:* Время загрузки игнорируем. Size подписи ~ 1 КБ. Время = 0,5 мс. (Если подпись индексного файла около 5 КБ, то 2,5 мс).

12. Задача: Злоумышленник изменил один бит в бинарном файле /bin/login. Размер файла 2 МБ. Как быстро подсистема ЗПС обнаружит подмену при попытке входа? *Ответ:* Мгновенно (при вызове `execve`), так как проверяется хеш-сумма всего файла целиком перед передачей управления коду.

13. Задача: Администратор отключил ЗПС (`astra-admin setzps off`) для установки драйвера. Система проработала 2 часа, затем ЗПС была включена обратно. Через какое время драйвер перестанет запускаться, если он не был подписан администратором локальным ключом? *Ответ:* Сразу же (при первой же попытке вызова драйвера после включения флага ЗПС).

14. Задача: Длина закрытого ключа RSA-2048 составляет 2048 бит. Сколько десятичных знаков (примерно) содержится в числе, составляющем этот ключ? (Использовать формулу $\log_{10}(2) \approx 0,3$). *Ответ:* $2048 \times 0,3 \approx 614$ знаков.

15. Задача: Для формирования доверенного канала связи используется алгоритм «Магма» в режиме гаммирования по ГОСТ Р 34.13-2015. Длина блока — 64 бита. Сколько блоков гаммы потребуется для зашифрования сетевого пакета MTU Ethernet (1500 байт)? *Ответ:* 1500 байт = 12 000 бит. $12\,000 / 64 = 187,5$. Округляем вверх — 188 блоков.

16. Задача: Срок действия сертификата открытого ключа пользователя истекает через 10 минут. Пользователь начал подписывать архив объемом 1 ГБ. Успеет ли он завершить процесс, если средняя скорость записи на диск 80 МБ/сек, а наложение подписи добавляет 5% накладных расходов к объему записываемых данных? *Ответ:* Время записи $\approx 1000 / 80 = 12,5$ сек. Даже с учетом криптографии это займет менее 20 секунд. *Ответ:* Да, успеет.

17. Задача: В алгоритме ГОСТ 28147-89 длина подключа раунда составляет 32 бита, всего раундов 32. Каков суммарный объем ключевого материала, циркулирующего внутри блочного шифра за один цикл (без учета мастер-ключа)? *Ответ:* $32 \times 32 = 1024$ бита (128 байт).

18. Задача: Утилита `ausearch` обрабатывает журнал аудита со скоростью 10 000 записей в секунду. Журнал содержит 50 миллионов записей об инциденте месячной давности. Сколько времени займет поиск нужного события? *Ответ:* $50\,000\,000 / 10\,000 = 5\,000$ сек (≈ 1 час 23 минуты).

19. Задача: Политика безопасности требует ротации паролей каждые 90 дней. Администратор установил параметр `PASS_MAX_DAYS` в файле `/etc/login.defs`. Какую команду необходимо выполнить, чтобы принудительно заставить пользователя `ivanov` сменить пароль при следующем входе, не меняя сам пароль? *Ответ:* `chage -d 0 ivanov`.

20. Задача: При загрузке Astra Linux SE выполняется self-test модулей СКЗИ. Время теста — 12 секунд. Общее время загрузки ОС до окна авторизации — 45 секунд. Каков процент задержки, вносимый требованиями безопасности (ФСТЭК)? *Ответ:* $(12 / 45) \times 100\% \approx 26,7\%$.

21. Задача: В системе включен МКЦ. Администратор (уровень целостности «Высокий») пытается удалить системную библиотеку `libc.so` (уровень целостности «Средний»). Получит ли он ошибку «Permission denied»? *Ответ:* Нет, удаление разрешено (высокий уровень целостности позволяет модифицировать объекты низкого уровня, защита работает в обратную сторону — низкий не может тронуть высокий).

22. Задача: Объем журнала `/var/log/parsec/` растет линейно на 50 МБ в час. Дисковое пространство раздела `/var` ограничено 10 ГБ и занято другими данными на 7 ГБ. Через сколько часов система аудита остановится из-за нехватки места (предполагая, что при заполнении диска сервис падает)? *Ответ:* Свободно 3 ГБ (3072 МБ). $3072 / 50 = 61,44$ часа.

23. Задача: Для обхода ЗПС злоумышленнику нужно внедрить библиотеку-посредник (`LD_PRELOAD`). Однако переменная окружения `LD_PRELOAD` очищается ядром при старте доверенных процессов. Каким образом ЗПС предотвращает использование этого вектора атаки даже при наличии уязвимости в приложении? *Ответ:* Путем очистки окружения и блокировки динамической подгрузки недоверенных ELF-секций на уровне ядра (через `ptrace restrictions` и проверку интерпретатора).

24. Задача: Два процесса обмениваются данными через разделяемую память (`shm`). Процесс А имеет метку {1}, процесс Б — {2}. Согласно правилам МКЦД, возможна ли прямая запись данных процессом А в сегмент памяти процесса Б? *Ответ:* Нет, запрещена правилом «No write down» (процесс с низким уровнем не может передавать информацию в область высокого уровня напрямую).

25. Задача: Вычислите энтропию пароля длиной 10 символов, состоящего только из строчных латинских букв (алфавит 26 символов). *Ответ:* $\$10 \times \log_2(26) \approx 10 \times 4,7 = 47$ бит.

26. Задача: Администратор назначает пользователю права `rwX` на файл через `chmod 777`. Поможет ли это пользователю прочитать файл, если метка безопасности файла {Особой важности}, а сессия пользователя {Секретно}? *Ответ:* Нет, механизмы DAC (`chmod`) подчиняются MAC (меткам). Нарушение иерархии уровней блокирует доступ раньше, чем проверяются права POSIX.

27. Задача: При печати документа на принтере срабатывает правило маркировки страниц. Если документ имеет метку «Для служебного пользования», какой элемент обязательно появится на каждом листе бумаги согласно стандартам делопроизводства РФ, реализуемым в CUPS-GOST? *Ответ:* Угловой штамп (реквизит 29 по ГОСТ Р 7.0.97-2016) или надпись в колонтитуле с указанием грифа.

28. Задача: Система использует аппаратный датчик случайных чисел (ГСЧ), выдающий 100 кбит истинно случайных данных в секунду. Сколько времени потребуется для генерации seed (зерна) длиной 256 бит для инициализации программного генератора `CSPRNG`? *Ответ:* $256 / 100\,000 = 0,00256$ сек.

29. Задача: В кластере виртуализации запущено 50 машин под управлением Astra Linux. Каждая машина отправляет heartbeat-сигнал (сигнал жизни) раз в 2 секунды размером 512 байт. Какова минимальная гарантированная полоса пропускания сети управления, необходимая только для поддержания связности кластера? *Ответ:* Один узел: $512 / 2 = 256$ байт/сек. Весь кластер: $\$256 \times 50 = 12\,800$ байт/сек (≈ 100 Кбит/сек).

30. Задача: Администратор случайно назначил метку «Открытые данные» файлу базы данных паролей. Система мониторинга (`MaxPatrol` или встроенный сканер) проводит проверку раз в сутки. Каково «окно уязвимости» (максимальное время), в течение которого критический файл остается без надлежащей защиты? *Ответ:* До 24 часов (интервал между сканированиями минус время, прошедшее с момента последнего сканирования до совершения ошибки).

2. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ТЕКУЩЕГО КОНТРОЛЯ

Вид контроля	Наименование работы	Наименование оценочных средств	Шкала оценивания
Текущий контроль	Вопросы для обсуждения на занятиях; Устные опросы по ранее изученному материалу; Письменные работы: рефераты, тестовые задания; Ситуационные и практические задания; Рефераты и доклады по темам (вопросам), вынесенным на самостоятельную работу.	Оценка выступлений на практическом (семинарском) занятии, проверка заданий и аудиторных работ, устный опрос, оценивание докладов, рефератов	отлично хорошо удовлетворительно неудовлетворительно

Критерии оценивания устных ответов обучающихся

Шкала оценивания	Характеристика оценивания
отлично	оценивается ответ, который показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа.
хорошо	оценивается ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.
удовлетворительно	оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа.
неудовлетворительно	оценивается ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа.

Критерии оценивания работы обучающихся на практических и семинарских занятиях

Шкала оценивания	Показатели	Критерии
Отлично	1. Полнота выполнения практического и тестового задания (полнота ответа); 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения практического задания (логичность и четкость ответа);	Задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом. Дан правильный и исчерпывающий ответ на поставленные теоретические и тестовые вопросы, в которых обучающийся показал всестороннее системное знание программного материала, усвоение основной и дополнительной литературы, четкое владение понятийным аппаратом.
Хорошо	4. Правильность ответов на вопросы; 5. Самостоятельность решения (владение дополнительным материалом); 6. Знание нормативно-законодательной базы и терминологии курса	Задание решено с помощью преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ. На поставленные теоретические и тестовые вопросы, при которых обучающийся показал достаточный уровень знаний основного программного материала: освоение информации лекционного курса и учебных пособий, овладение понятийным аппаратом, методикой исследований при попытке анализа различных ситуаций.
Удовлетворительно		Задание решено с подсказками преподавателя. Задание решено в общем виде. Обучающийся показал средний уровень знаний основного программного материала, но не мог убедительно аргументировать свой ответ, ошибся в использовании понятийного аппарата, показал недостаточные знания литературных источников.
Неудовлетворительно		Задание не решено. Обучающийся продемонстрировал значительные пробелы в знаниях основного программного материала, не аргументировал свой ответ, показал неудовлетворительные знания понятийного аппарата и специальной литературы.

Критерии оценивания рефератов

Форам контроля	Критерии оценивания	Шкала оценивания
Реферат	Выполнены все методические требования к написанию реферата: определена тема, актуальность; содержание соответствует теме и плану реферата; сделан краткий анализ различных точек зрения по рассматриваемой проблеме;	зачтено

	грамотно использованы первоисточники при анализе содержания; выводы сформулированы лаконично с логическими доказательствами; соблюдены требования по внешнему оформлению. Тема реферата раскрыта в полном объеме.	
	Нарушены требования по написанию и оформлению реферата. Несоответствие темы реферата. В тексте не отражены существенные моменты. Тема реферата не раскрыта до конца. Сделаны необоснованные выводы.	не зачтено

Критерии оценивания тестов

Средство контроля	Критерии оценивания – процент положительных ответов	Шкала оценивания
Тестирование	90-100	отлично
	70-89	хорошо
	40-69	удовлетворительно
	< 39	неудовлетворительно

3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Средства оценивания в ходе промежуточной аттестации:

- вопросы для зачета;
- практические задания для зачета.

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

3.1. Вопросы к зачёту

1. Сущностно-ролевая ДП-модель управления доступом: определение субъекта, объекта, сущности и метки безопасности в контексте PARSEC.
2. Правила доминирования меток конфиденциальности при чтении и записи данных. Примеры ситуаций предоставления и отказа в доступе.
3. Иерархические уровни конфиденциальности и неиерархические категории секретности: структура, назначение и правила комбинирования.

4. Наследование меток безопасности при создании новых объектов файловой системы. Как определяется начальная метка файла?
5. Механизм предотвращения утечки конфиденциальной информации («запись вниз») и его отличие от классической модели Белла — Лападулы.
6. Особенности работы с несекретными данными (нулевой уровень) в сессии пользователя с ненулевым уровнем допуска.
7. Влияние мандатного контроля на межпроцессное взаимодействие (IPC) и использование разделяемой памяти.
8. Понятие «доверенный процесс» в Astra Linux SE и механизм игнорирования правил МКЦД для системных служб.
9. Отличия реализации мандатного контроля в режимах функционирования ОС «Базовый», «Усиленный» и «Максимальный».
10. Назначение мандатного контроля целостности (МКЦ). Уровни целостности субъектов и объектов.
11. Механизм заморозки процесса (*freeze*): причины срабатывания, влияние на графическую сессию пользователя и способы диагностики.
12. Изоляция процессов с использованием пространств имен (*namespaces*) и её роль в предотвращении горизонтального перемещения злоумышленника.
13. Модель Privileged User Identity (PUI): отказ от использования учетной записи *root* и механизмы делегирования привилегий через *sudo* и политики безопасности.
14. Взаимодействие уровней целостности и уровней конфиденциальности: как они дополняют друг друга в защите ядра ОС.
15. Механизмы защиты стека и кучи исполняемых процессов (ASLR, NX-bit) в связке с аппаратными средствами доверенной загрузки.
16. Принципы работы ЗПС: электронная подпись исполняемых файлов и разделяемых библиотек. Форматы контейнеров подписи (*.sig*).
17. Последствия нарушения целостности бинарного файла или его цифровой подписи при попытке запуска в среде с активной ЗПС.
18. Управление локальными ключами администратора для подписания стороннего программного обеспечения. Утилиты *gostsum*, *fly-digisign*.
19. Влияние ЗПС на работу пакетного менеджера АРТ: проверка подписей репозитория и пакетов *.deb*.
20. Режим мягкого и жесткого блокирования ЗПС: различия в поведении системы при обнаружении недоверенного кода.
21. Интеграция СКЗИ (например, КриптоПро CSP) с системными компонентами Astra Linux: работа со считывателями, контейнерами ключей и сертификатами X.509.
22. Обеспечение электронной подписи документов на уровне пользовательского графического интерфейса (*Cedar Office*, *Fly-Filer*) и командной строки.
23. Организация защищенных каналов связи (VPN) с использованием ГОСТ-алгоритмов шифрования в составе дистрибутива.
24. Шифрование носителей информации (жестких дисков, флеш-накопителей) штатными средствами LUKS с поддержкой отечественных стандартов.
25. Требования к хранению закрытых ключей пользователей: сравнение программных токенов, реестра и аппаратных носителей (Рутокен, JaCarta).
26. Подсистема аудита безопасности: формат записей, основные классы событий (LOGIN, MAC_POLICY, EXECVE).
27. Централизованный сбор журналов безопасности (*auditd*, *syslog-ng*). Настройка пересылки логов на удаленный сервер во избежание их модификации злоумышленником.
28. Утилиты анализа журналов (*ausearch*, *aureport*). Поиск следов несанкционированного повышения привилегий.
29. Контроль целостности файловой системы в режиме реального времени (AIDE): принцип работы, база снимков и реакция на инциденты.

30. Специфика регистрации событий при работе с объектами нулевой метки в высокоуровневой сессии: почему эти события критичны для расследования инцидентов?

3.2. Практические задания к зачёту

1. **Задача:** Алгоритм ГОСТ Р 34.10-2012 выполняет формирование электронной подписи для документа объемом 1 МБ за 40 миллисекунд. Рассчитайте максимальную пропускную способность сервера в операциях подписания в секунду. (Решение: $1 / 0,04 \text{ сек} = 25 \text{ операций/сек}$)
2. **Задача:** Аппаратный токен «Рутокен ЭЦП» выполняет хеширование данных по алгоритму ГОСТ Р 34.11-2012 («Стрибог-256») за 8 миллисекунд. Какова максимальная скорость обработки запросов данным устройством? (Решение: $1 / 0,008 \text{ сек} = 125 \text{ операций/сек}$)
3. **Задача:** Межсетевой экран на базе Astra Linux расшифровывает входящие IPsec-пакеты (ГОСТ Р 34.12-2015 «Магма»). Время обработки одного пакета составляет 2 миллисекунды. Определите максимальное количество пакетов, которое устройство может обработать за одну секунду без потерь. (Решение: $1 / 0,002 \text{ сек} = 500 \text{ пакетов/сек}$)
4. **Задача:** Процедура проверки целостности загрузчика GRUB и ядра Linux с использованием ПАК СЗИ «Соболь» занимает 3 секунды при каждой перезагрузке сервера. Если сервер планово перезагружается один раз в месяц (30 дней), какую долю времени от общего месяца (в процентах) занимает процедура доверенной загрузки? Округлить до четырех знаков после запятой. (Решение: $(3 / (30 * 24 * 3600)) * 100 \approx 0,0001\%$)
5. **Задача:** Система аудита безопасности генерирует события со скоростью 200 записей в секунду. Средний размер одной записи — 512 байт. Вычислите минимальный объем дискового пространства (в мегабайтах), необходимый для хранения журнала за одни сутки бесперебойной работы. (Решение: $200 * 512 * 86400 / (1024 * 1024) \approx 8203 \text{ МБ}$)
6. **Задача:** Пользователь работает в сессии с меткой конфиденциальности {Уровень 2}. Он пытается скопировать файл из своей домашней директории (наследование уровня {Уровень 2}) на USB-накопитель, который автоматически смонтировался с меткой {Уровень 1} согласно политике мандатного контроля. Опишите состояние процесса копирования сразу после запуска. (Решение: Процесс будет заблокирован/заморожен ядром PARSEC из-за нарушения правила «запись вниз»).
7. **Задача:** Замкнутая программная среда (ЗПС) проверяет электронную подпись исполняемого файла перед запуском. Скорость верификации подписи составляет 50 файлов в секунду. Сколько максимум новых процессов сможет запустить пользователь за 10 секунд, если ЗПС активна? (Решение: $50 * 10 = 500 \text{ процессов}$)
8. **Задача:** Длина закрытого ключа RSA-4096 составляет 4096 бит. При передаче этого ключа по защищенному каналу он упаковывается в контейнер формата PKCS#8, добавляя к исходным данным 256 байт служебной информации (OID алгоритма, версия). Каков итоговый размер контейнера в байтах? (Решение: $4096 / 8 + 256 = 512 + 256 = 768 \text{ байт}$)
9. **Задача:** Администратор меняет пароль пользователя. Новый пароль должен пройти проверку сложности модулем pam_pwquality. Проверка одного пароля занимает 15 микросекунд. Сколько паролей сможет проверить система за 1 секунду при подборе (brute-force)? (Решение: $1 / 0,000015 \text{ сек} \approx 66\,666 \text{ паролей/сек}$)
10. **Задача:** В системе Astra Linux включен режим очистки памяти (memory sanitization) при освобождении страниц процессами. Скорость заполнения освобождаемой памяти нулями составляет 2 ГБ в секунду. Сколько времени займет

- очистка адресного пространства завершеного приложения размером 1,5 ГБ?
(Решение: $1,5 / 2 = 0,75$ сек)
11. **Задача:** Сервер VDI (Virtual Desktop Infrastructure) на базе Astra Linux поддерживает 50 одновременных сессий. Каждой сессии требуется обновление экрана (кадров) частотой 1 раз в 50 миллисекунд. Рассчитайте общую частоту генерации кадров сервером в секунду. (Решение: $50 * (1 / 0,05) = 1000$ кадров/сек)
 12. **Задача:** Криптопровайдер КриптоПро CSP вычисляет ключ согласования по протоколу Диффи — Хеллмана за 12 миллисекунд. Рассчитайте, сколько TLS-рукопожатий (handshake) в секунду может выполнить веб-сервер под высокой нагрузкой. (Решение: $1 / 0,012$ сек ≈ 83 операции/сек)
 13. **Задача:** Файл имеет метку {Особой важности, КБ}. У пользователя сессия {Секретно, КБ, КТ}. Сможет ли пользователь прочитать файл согласно правилам доминирования МКЦД? (Решение: Нет, так как уровень сессии «Секретно» ниже уровня файла «Особой важности»).
 14. **Задача:** Демон автоматического обновления fly-admin-update-checker опрашивает репозиторий каждые 4 часа. Каждое сканирование занимает ровно 2 минуты. Какую долю времени (в процентах) процесс опроса занимает в течение полных суток? (Решение: $(6 \text{ проверок} * 120 \text{ сек}) / 86400 \text{ сек} * 100 \approx 0,083\%$)
 15. **Задача:** При печати конфиденциального документа CUPS-сервер накладывает водяной знак (watermark) поверх текста. Рендеринг водяного знака замедляет печать страницы на 200 миллисекунд. На сколько процентов увеличится время печати партии из 100 страниц по сравнению с обычной печатью, если базовая скорость принтера — 1 страница в секунду? (Решение: Базовое время 100 сек. Задержка $100 * 0,2 = 20$ сек. Итого 120 сек. Увеличение на 20%).
 16. **Задача:** Алгоритм блочного шифрования «Кузнечик» обрабатывает данные блоками по 128 бит. Чтобы зашифровать видеопоток скоростью 768 килобит в секунду, сколько блоков должен обрабатывать процессор каждую секунду (без учета накладных расходов)? (Решение: $768\,000 / (128 / 8) = 48\,000$ блоков/сек)
 17. **Задача:** Утилита `pdpl -l` выводит список всех доступных уровней секретности. Если вывод этой команды задерживается на 50 миллисекунд из-за обращения к медленному сетевому хранилищу меток, а скрипт вызывает её 200 раз подряд, на сколько секунд дольше отработает скрипт по сравнению с работой из оперативной памяти? (Решение: $0,05 * 200 = 10$ сек)
 18. **Задача:** Емкость аппаратного модуля TPM (Trusted Platform Module) для сохранения измерений целостности (PCR) ограничена. Если каждое измерение ПО добавляет 20 байт данных в лог загрузки, а выделенный буфер составляет 160 байт, сколько компонентов системы успеет измерить модуль до его переполнения? (Решение: $160 / 20 = 8$ компонентов)
 19. **Задача:** Сессия SSH с использованием алгоритмов ГОСТ устанавливается за 3 последовательных этапа обмена пакетами. Каждый этап требует 10 мс на вычисления и 30 мс на передачу по сети с учетом задержки (latency). Найдите общее время установления соединения. (Решение: $3 * (10 + 30) = 120$ мс)
 20. **Задача:** Подсистема AIDE (Advanced Intrusion Detection Environment) проверяет целостность 10 000 системных файлов. На расчет контрольной суммы одного файла уходит 2 миллисекунды. Рассчитайте минимальное время полной проверки всей системы. (Решение: $10\,000 * 0,002 = 20$ сек)
 21. **Задача:** Пользователь пытается повысить свой мандатный уровень через утилиту `pdpl-user` с «Для служебного пользования» на «Секретно». Система запрашивает подтверждение администратора безопасности. Ответ от администратора приходит через сеть за 1,5 секунды. Если операционная система делает три попытки запроса подтверждения перед отказом, каково максимальное ожидание пользователя? (Решение: $1,5 * 3 = 4,5$ сек)

22. **Задача:** Ширина канала связи между двумя ЦОД составляет 100 Мбит/с. Канал полностью зашифрован алгоритмом AES-256-GCM. Если шифрование нагружает процессор шлюза так, что эффективная скорость падает до 70 Мбит/с, вычислите потери производительности в процентах. (Решение: $((100 - 70) / 100) * 100 = 30\%$)
23. **Задача:** В модуле ЗПС используется кэш проверенных подписей. Время жизни записи в кэше — 60 секунд. Если приложение запускается 10 раз в минуту, и каждый запуск без кэша занимает 100 мс, а из кэша — 1 мс, сколько процессорного времени (в секундах) экономится за счет кэширования за эту минуту? (Решение: 1 запуск без кэша (первый): 0,1 сек. Остальные 9: $9 * (0,1 - 0,001) = 0,891$ сек. Итого экономия: 0,891 сек).
24. **Задача:** Длина серийного номера сертификата X.509 составляет 20 байт. Какое количество уникальных сертификатов может выпустить удостоверяющий центр, прежде чем вероятность коллизии (по парадоксу дней рождения) превысит 50%? (Для оценки использовать упрощенную формулу $\sqrt{2^n}$). (Решение: 2^{160} вариантов. $\sqrt{2^{160}} = 2^{80}$)
25. **Задача:** Процесс-демон потребляет 10% CPU при работе. Каждые 5 минут он выполняет операцию переключивания журналов (logrotate), которая длится 30 секунд и потребляет 80% CPU. Какова средняя загрузка CPU этим процессом за час? (Решение: Активная фаза: $(12 \text{ раз} * 30 \text{ сек}) * 0,8 = 288 \text{ сек-значений}$. Пассивная фаза: $(3600 - 360) \text{ сек} * 0,1 = 324 \text{ сек-значений}$. Среднее: $(288 + 324) / 3600 \approx 17\%$).
26. **Задача:** При включенном мандатном контроле целостности (МКЦ) ядро проверяет права доступа к каждому системному вызову `open()`. Это добавляет задержку в 5 микросекунд на каждый вызов. Если база данных совершает 50 000 таких вызовов в секунду, какая часть ресурсов CPU (в процентах) тратится исключительно на эти проверки? (Решение: $50\,000 * 0,000005 = 0,25 \text{ сек}$. Из одной секунды это 25%).
27. **Задача:** Объем дистрибутива ОС Astra Linux Special Edition составляет 6,5 ГБ. Для его скачивания используется канал со скоростью 50 Мбит/с. Однако из-за работы встроенного межсетевого экрана каждая порция данных (MTU) задерживается на 0,5 мс. При MTU 1500 байт рассчитайте реальное время скачивания образа. (Решение: Количество пакетов = $(6,5 * 1024 * 1024 * 8) / (1500 * 8) \approx 3641$ пакетов. Только задержка: $3641 * 0,0005 = 1,82 \text{ сек}$. Чистое время передачи: $(6,5 * 8) / 50 = 1,04 \text{ сек}$. Итого $\sim 2,86 \text{ сек}$).
28. **Задача:** Алгоритмы ГОСТ работают в режиме сцепления блоков (CBC). Вектор инициализации (IV) обновляется для каждого нового сообщения. Если генерация криптографически стойкого IV занимает 0,2 миллисекунды, сколько сообщений можно инициировать в секунду? (Решение: $1 / 0,0002 \text{ сек} = 5000 \text{ сообщений/сек}$)
29. **Задача:** Журнал `/var/log/auth.log` растет со скоростью 2 МБ в минуту. Диск раздела `/var` имеет объем 20 ГБ и заполнен другими данными на 19 ГБ. Через какое время (в минутах) служба входа перестанет фиксировать события из-за нехватки места? (Решение: Свободно 1024 МБ. $1024 / 2 = 512 \text{ минут}$).
30. **Задача:** Для обхода блокировки неизвестного ПО администратор добавляет хеш-сумму файла в белый список ЗПС. Запись одного хеша в базу данных `parsec` выполняется транзакцией SQLite за 0,5 миллисекунды. Сколько максимум приложений администратор может добавить в доверенную зону за 10 секунд рабочего времени? (Решение: $10 / 0,0005 = 20\,000 \text{ приложений}$)

4. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Шкала оценивания уровня сформированности профессиональных компетенций (зачет)

Шкала оценивания	Уровень освоение компетенции	Критерии оценивания
Зачет	Базовый уровень освоения компетенции	Дан правильный и исчерпывающий ответ на вопрос. Обучающийся демонстрирует знание теоретического материала, изложено правильное понимание вопроса, дано достаточно подробное описание предмета ответа, приведены и раскрыты в тезисной форме основные понятия, относящиеся к предмету ответа. Обучающимся усвоена взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии. Имеется базовый уровень овладения практическими умениями и навыками по данной дисциплине в соответствии с ФГОС .
Незачет	Неудовлетворительный уровень	Отсутствует ответ или в ответе есть грубые ошибки, свидетельствующие о отсутствии знаний соответствующего программного материала; отсутствие умений и навыков по данной дисциплине в соответствии с ФГОС и/или фрагментарные знания основного учебно-программного материала.

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.