Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Алтайский государственный университет»
международный институт экономики, менеджмента и информационных систем
Кафедра прикладной информатики в экономике, государственном и муниципальном управлении

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Информационная безопасность»

09.03.03. Прикладная информатика
«Цифровая экономика»

Разработчик:
к.ф.-м.н., доцент кафедры прикладной информатики в экономике, государственном и муниципальном управлении

/О. В. Журенков/

Барнаул, 2020

Визирование ФОС для исполнения в очередном учебном году

Фонд оценочных средств пересмотрен, обсуждён и одобрен для исполнения в 2020–2021 учебном году на заседании кафедры прикладной информатики в экономике, государственном и муниципальном управлении.

Внесены следующие изменения и дополнения:

Протокол от 14.05.2020 № 10
Зав. кафедрой А. Ю. Юдинцев, доцент

ПАСПОРТ КОМПЛЕКТА ОЦЕНОЧНЫХ СРЕДСТВ

1. Перечень формируемых компетенций:

- ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
- ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью.
- ПК-1: Способен проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе.
- ПК-3: Способен проектировать ИС по всем видам обеспечения.
- ПК-10: Способен принимать участие в организации ИТ- инфраструктуры и управлении информационной безопасностью.

2. Планируемые результаты освоения дисциплины:

№ п/п	Контролируемые разделы дисциплины	Код контролируемой компетенции (или её части)	Код и наименование индикатора достижения	Наименование оценочного средства
1.	Раздел 1. Введение в информационную безопасность	ОПК-3, ПК-10	• ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. • ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. • ПК-10.1. Знать виды и способы формирования организационных структур информационной службы; международные стандарты управления автоматизированными информационными системами и информационной службой предприятия.	Практические задания к лабораторным работам. Тест.

2.	Раздел 2. Программно-технический уровень информационной безопасности	ОПК-3, ПК-1, ПК-3, ПК-10	• ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. • ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. • ПК-1.2. Уметь проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе. • ПК-3.1. Знать методы и технологии проектирования ИС по видам обеспечения. • ПК-3.2. Уметь применять методы и технологии проектирования ИС по видам обеспечения. • ПК-10.1. Знать виды и способы формирования организационных структур информационной службы; международные стандарты управления автоматизированными информационными системами и информационной службой предприятия. • ПК-10.2. Уметь формулировать требования бизнеса и цели внедрения автоматизированной информационной системы; грамотно оценивать затраты, связанные с разработкой, внедрением.	Практические задания к лабораторным работам. Тест.

3.	Раздел 3. Законодательный и административный уровни информационной безопасности	ОПК-3, ОПК-4, ПК-1, ПК-10	• ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. • ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. • ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. • ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы. • ПК-1.2. Уметь проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе. • ПК-10.1. Знать виды и способы формирования организационных структур информационной службы; международные стандарты управления автоматизированными информационными системами и информационной службой предприятия. • ПК-10.2. Уметь формулировать требования бизнеса и цели внедрения автоматизированной информационной системы; грамотно оценивать затраты, связанные с разработкой, внедрением.	Практические задания к лабораторным работам. Тест.

4.	Промежуточная аттестация по дисциплине — экзамен	ОПК-3, ОПК-4, ПК-1, ПК-3, ПК-10	• ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. • ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. • ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. • ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы. • ПК-1.2. Уметь проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе. • ПК-3.1. Знать методы и технологии проектирования ИС по видам обеспечения. • ПК-3.2. Уметь применять методы и технологии проектирования ИС по видам обеспечения. • ПК-10.1. Знать виды и способы формирования организационных структур информационной службы; международные стандарты управления автоматизированными информационными системами и информационной службой предприятия. • ПК-10.2. Уметь формулировать требования бизнеса и цели внедрения автоматизированной информационной системы; грамотно оценивать затраты, связанные с разработкой, внедрением.	Тест.

3. Типовые оценочные средства, необходимые для оценки планируемых результатов обучения по дисциплине:

ТЕКУЩИЙ КОНТРОЛЬ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ОЦЕНОЧНОЕ СРЕДСТВО-1: Практические задания к лабораторным работам

1. **Цель:** Практические задания к лабораторным работам представляют собой пошаговую инструкцию к выполнению лабораторных работ, содержащих требования практического характера и сопутствующие вопросы, для контроля понимания теоретического материала и степени овладения практическим навыками. Ответ предоставляется в форме отчёта.

2. **Контролируемый раздел дисциплины:** Раздел 1. Введение в информационную безопасность; Раздел 2. Программно-технический уровень информационной безопасности; Раздел 3. Законодательный и административный уровни информационной безопасности.

3. **Проверяемые компетенции (код):** ОПК-3, ОПК-4, ПК-1, ПК-3, ПК-10.

4. **Индикаторы достижения:**

   - ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
   - ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
   - ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
   - ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.
   - ПК-1.2. Уметь проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе.
   - ПК-3.1. Знать методы и технологии проектирования ИС по видам обеспечения.
   - ПК-3.2. Уметь применять методы и технологии проектирования ИС по видам обеспечения.
   - ПК-10.1. Знать виды и способы формирования организационных структур информационной службы; международные стандарты управления автоматизированными информационными системами и информационной службой предприятия.
   - ПК-10.2. Уметь формулировать требования бизнеса и цели внедрения автоматизированной информационной системы; грамотно оценивать затраты, связанные с разработкой, внедрением.

5. **Пример оценочного средства: Лабораторная работа №1**

   Создание безопасной экспериментальной среды

   Для создания безопасной экспериментальной среды можно использовать выделенные компьютеры (не включённые в корпоративную сеть), однако более удобным решением, в современных условиях, является создание такой среды на основе виртуализации. Сейчас даже на рабочих станциях можно запустить несколько виртуальных машин.

   Для создания полноценной среды необходимо развернуть *сетевую* ОС с *серверными службами*. Поэтому необходимо создать виртуальную машину с ОС семейства GNU/Linux. В данных условиях Вы можете установить ОС Ubuntu (репозиторий поддерживается управлением информатизации АлтГУ) или ОС Rosa (репозиторий поддерживается кафедрой ПИЭГМУ МИЭМИС АлтГУ).

Задание 1. Создание виртуальной машины

Используя VirtualBox создайте и настройте новую виртуальную машину.

5.1. Работая в компьютерном классе, проверьте, имеется ли в директории `D:\ISO`[1] образ диска с дистрибутивом ОС, посмотрите, как называется эта операционная система. Скопируйте в директорию `D:\ISO` образ диска с дистрибутивом ОС (файл `ROSA.FRESH.KDE4.R11.x86_64.uefi.iso`) с ресурса ftp://piegmu.asu.ru/. Если на ПК имеется скачанный дистрибутив предыдущей версии, можно использовать его. При наличии опыта работы в GNU/Linux Вы можете использовать дистрибутив `Ubuntu`, `Debian` или `Linuxmint` (для этих ОС поддерживаются репозитории в АлтГУ)

5.2. Запустите VirtualBox, посмотрите настройки (▷ Файл ▶ Свойства), обратите внимание на *Хост-клавишу*. Посмотрите, куда сохраняются виртуальные машины. Если работаете в компьютерном классе, то задайте папку для машин `D:\`.

5.3. Создайте новый образ виртуальной машины для *Вашей* ОС, например:

Имя — ROSA-2021-фамилия;
Операционная система — Linux;
Версия — Mandriva 64.

Внимательно прочитайте рекомендации мастера, используйте свойства по умолчанию, предлагаемые мастером, кроме двух:

тип жёсткого диска — Virtual Machine Disk (VMDK);
размер — 20 ГБ.

5.4. Посмотрите *свойства* полученного образа. Увеличьте размер *основной памяти* до 1024 МБ (можно больше, но не более половины от доступной памяти). Если есть возможность, увеличьте число процессоров до 1/2 от доступного количества. Размер *видеопамяти* увеличьте (тоже до 1/2 от доступной).

5.5. Уберите из загрузочных устройств FDD («дискета») и свяжите с приводом оптических дисков скачанный ISO-образ с дистрибутивом (расположенным в `D:\ISO`). Если на компьютере есть аудиокарта, то выберите на вкладке Аудио Аудиоконтроллер `Intel HD Audio`.

5.6. Посмотрите «сетевые адаптеры», выберите тип подключения `Сетевой мост`. Добавьте ещё один сетевой адаптер, выберите для него тип подключения `NAT`.

Задание 2. Установка ОС

5.1. Запустите созданную виртуальную машина. По нажатию F12 можно изменить источник загрузки.

5.2. Следуя руководству мастера, установите гостевую ОС. Для управления устройствами виртуальной машины можно использовать меню или пиктограммы внизу окна.

Будьте внимательны, **пароль Администратора (root), задаваемый в конце установки ОС подлежит надёжному хранению**, т. к. в случае утери восстановлению/изменению не подлежит. Потребуется переустановка ОС!

5.3. Зайдите в гостевую ОС и посмотрите установленные компоненты.

Задание 3. Работа с виртуальной машиной и гостевой ОСGNU/Linux

5.1. Установите общий буфер обмена в режим двунаправленный (на вкладке Дополнительно в Общих ▷ свойствах виртуальной машины).

5.2. Проверьте работу сети гостевой ОС, при необходимости измените настройки виртуальной сетевой карты.

5.3. Посмотрите возможности настройки ОС (через пиктограмму в панели быстрого запуска).

5.4. Добавьте пользователя `user` с паролем `user` (отдельную группу создавать не надо).

5.5. Внимание, этот пункт выполняется только в локальной сети АлтГУ!

Для ОС Rosa, запустите **менеджер источников программ**, отключите все включенные источники и добавьте (через меню ▶ Файл) *пользовательский источник* (для Rosa):

[1] Если отсутствует диск `D:`, используйте каталог `C:\VirtualBox`.

- тип — Сервер HTTP;
- URL — http://piegmu.asu.ru/rosa/;
- включите все переключатели.

После добавления этого репозитория появится сообщение об ошибке, связанной с невозможностью добавить 32-разрядный репозиторий (ничего страшного, этого репозитория действительно нет).

5.6. Внимание, этот пункт выполняется только в локальной сети АлтГУ!

Для других ОС (`Ubuntu`, `Debian`, `Linuxmint`), следуйте указаниям, приведённым на http://linuxupdate.asu.ru/.

5.7. Выполните обновление системы.

5.8. Установите систему управлениями проектами Planner, редактор BlueFish и ещё какой-нибудь софт по желанию (например, игру).

5.9. Посмотрите оборудование виртуальной машины.

5.10. Посмотрите в VirtualBox, как работает Ваша машина. Сделайте *снимок* машины.

5.11. Измените настройки рабочего стола, окон. Можете даже «сломать» машину.

5.12. Выключите машину (можно аварийным способом). Восстановите состояние машины из снимка.

5.13. Создайте и подключите «общую папку». Для подключения используйте (из-под root) `mount -tvboxsf папка точкаМонтирования`, где `папка` — название общей папки в VirtualBox, а `точкаМонтирования` может быть любой доступной директорией в гостевой ОС, например в Вашей домашней директории или `/mnt`.

Для работы с общими папками на Linux необходимо внести пользователя гостевой системы в группу `vboxsf` Для подключения в виртуальной машине портов USB необходимо добавить пользователя хост-системы в группу vboxusers. Для включения режима USB 2.0 и USB 3.0 необходимо установить VirtualBox Extension Pack с сайта https://www.virtualbox.org/.

Задание 4. Пользовательские настройки OCGNU/Linux

5.1. Познакомьтесь с интерфейсом.

5.2. Изучите пиктограммы быстрого запуска и пиктограммы запущенных программ (в трэе).

5.3. Посмотрите оборудование компьютера.

5.4. Настройте раскладку клавиатуры (включите флаг страны).

5.5. Добавьте в панель быстрого запуска виджет «Классическое меню запуска приложений».

5.6. Измените настройки рабочего стола, окон. Увеличьте число рабочих столов до 4–6.

5.7. Посмотрите и настройте графические эффекты рабочего стола.

Задание 5. Работа с файлами в GNU/Linux

5.1. Используя Dolphin (также доступен из панели быстрого запуска), посмотрите имеющиеся ресурсы, сделайте вид «две панели» (F3).

5.2. Перейдите в домашнюю директорию, посмотрите скрытые файлы (Alt+.), воспользуйтесь фильтром (Ctrl+I).

5.3. Включите терминал в Dolphin (F4), посмотрите процессы (`ps`), посмотрите справку по этой команде (`ps --help`).

5.4. Можно выполнить и сохранить необходимые настройки Dolphin через меню ▷ Настройка ▶ Настроить Dolphin.

5.5. Узнайте (в Windows) полное название сетевых дисков (`P:`, `U:`) и подключите эти ресурсы, используя Dolphin. Для удобства можно добавить часто используемые ресурсы в «точки входа».

5.6. Попробуйте скопировать *окно*, вставить изображение в документ, сохранить этот документ в формате PDF.

5.7. Создайте в другой папке ссылку на этот документ. Откройте файл-ссылку, измените, сохраните и закройте. Откройте оригинальный файл, посмотрите изменения.

5.8. Запустите консоль. Определите своё местонахождение в файловой системе (`pwd`). Посмотрите список файлов (`ls`). Посмотрите подсказку по команде (например, `ls --help`). Посмотрите документацию (manual) по команде. (например, `man ls`).

5.9. Запустите консольный файловый менеджер Midnight Commander (`mc`). Изучите доступные команды.

Задание 6. Работа группы виртуальных машин

5.1. Узнайте у одногруппников адреса их виртуальных машин.

5.2. Установите сетевое взаимодействие с другими виртуальными машинами в классе. Для этого можно предоставить общий доступ к некоторой папке на своей машине и зайти на такой же ресурс, предоставленной на другой машине.

5.3. Зайдите на чужую машину под логином `user`.

5.4. Попробуйте зайти на чужую машину под суперпользователем.

5.5. Попробуйте выключить чужую машину.

5.6. Выключите свою виртуальную машину.

6. **Критерии оценивания:** Для оценивания выполнения практических заданий применяются следующие показатели:

6.1. полнота выполнения задания;

6.2. своевременность выполнения задания;

6.3. логическая последовательность и рациональность выполнения задания;

6.4. уровень самостоятельности выполнения задания;

6.5. уровень творчества и новаторства при выполнении задания.

В соответствии с этими показателями, на основе табл. 2 выставляется оценка за каждое выполненное задание.

7. **Рекомендуемый перечень вопросов для самостоятельной подготовки:**

7.1. Понятие информационной безопасности. Основные составляющие информационной безопасности.

7.2. Основные угрозы информационной безопасности. Основные понятия.

7.3. Наиболее распространённые угрозы доступности.

7.4. Основные угрозы целостности.

7.5. Основные угрозы конфиденциальности.

7.6. Вредоносное программное обеспечение. Основные понятия.

7.7. Классификация вредоносных программ.

7.8. Способы защиты от вредоносных программ.

7.9. Программно-технический уровень информационной безопасности. Основные понятия.

7.10. Особенности современных информационных систем.

7.11. Архитектурная безопасность.

7.12. Управление доступом. Идентификация и аутентификация.

7.13. Авторизация.

7.14. Протоколы AAA.

7.15. Протоколирование и аудит. Основные понятия.

7.16. Активный аудит

7.17. Шифрование. Основные понятия.

7.18. Обеспечение конфиденциальности. Симметричное шифрование.

Таблица 2.

Оценивание выполнения практических заданий

4-балльная шкала (уровень освоения)	**100-балльная шкала**	**Критерии**
Отлично (повышенный уровень)	90–100	Студентом задание выполнено самостоятельно и в срок. При этом составлен правильный алгоритм выполнения задания, в логических рассуждениях, в выборе ПО и методах его применения нет ошибок, получен верный ответ, задание выполнено рациональным способом.
Хорошо (базовый уровень)	70–89	Студентом задание выполнено с небольшими подсказками преподавателя, возможно, с небольшой задержкой сроков. При этом составлен правильный алгоритм выполнения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор ПО и методов его применения для выполнения задания; есть объяснение выполнения, но задание выполнено не рациональным способом или допущено не более двух несущественных ошибок, получен верный ответ.
Удовлетворительно (пороговый уровень)	50–69	Студентом задание выполнено с подсказками преподавателя, с большой задержкой сроков. При этом задание понято правильно, в логическом рассуждении нет существенных ошибок, но, возможно, допущены существенные ошибки в выборе ПО и методов его применения или в составлении документации; задание выполнено не полностью или в общем виде.
Неудовлетворительно (уровень не сформирован)	0–49	Студентом задание не выполнено.

7.19. Обеспечение конфиденциальности. Асимметричное шифрование.

7.20. Контроль целостности. Электронная цифровая подпись. Цифровые сертификаты.

7.21. Административный уровень информационной безопасности. Основные понятия. Комплексная система защиты информации.

7.22. Политика безопасности.

7.23. Программа безопасности.

7.24. Синхронизация программы безопасности с жизненным циклом ИС.

7.25. Законодательный уровень информационной безопасности. Основные понятия.

7.26. Закон «Об информации, информатизации и защите информации».

7.27. Закон «О лицензировании отдельных видов деятельности».

7.28. Закон «Об участии в международном информационном обмене».

7.29. Закон «Об электронной цифровой подписи».

7.30. Нормативные документы.

ОЦЕНОЧНОЕ СРЕДСТВО-2: Тест

1. **Цель:** Набор тестовых вопросов разного типа служит для контроля степени усвоения теоретических знаний по каждой теме, уровень усвоения $\geqslant 50\%$ является условием для допуска к выполнению лабораторных работ по данной теме и/или к следующему разделу дисциплины.

2. **Контролируемый раздел дисциплины:** Раздел 1. Введение в информационную безопасность; Раздел 2. Программно-технический уровень информационной безопасности; Раздел 3. Законодательный и административный уровни информационной безопасности.

3. **Проверяемые компетенции (код):** ОПК-3, ПК-3, ПК-10.

4. **Индикаторы достижения:**

- ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
- ПК-3.1. Знать методы и технологии проектирования ИС по видам обеспечения.
- ПК-10.1. Знать виды и способы формирования организационных структур информационной службы; международные стандарты управления автоматизированными информационными системами и информационной службой предприятия.
- ПК-10.2. Уметь формулировать требования бизнеса и цели внедрения автоматизированной информационной системы; грамотно оценивать затраты, связанные с разработкой, внедрением.

5. Пример оценочного средства:

5.1. Все угрозы возникают вследствие каких-то ошибок или просчётов персонала. Выберите один ответ:
- Верно
- Неверно

5.2. Самыми частыми и самыми опасными угрозами доступности являются стихийные бедствия (пожары, наводнения и т.п.). Выберите один ответ:
- Верно
- Неверно

5.3. Как называется субъект, предпринявший попытку нарушения информационной безопасности?
Ответ:

5.4. Раскрытие предметной информации более опасно, чем раскрытие служебной информации. Выберите один ответ:
- Верно
- Неверно

5.5. Отметьте угрозы, которые можно отнести к угрозам конфиденциальности. Выберите один или несколько ответов:
- нанесение ущерба при сервисном обслуживании
- кража данных
- невозможность работать с системой в силу отсутствия соответствующей подготовки
- злоупотребление полномочиями
- отказы программного и аппаратного обеспечения
- изменение данных

5.6. Как называется потенциальная возможность определённым образом нарушить информационную безопасность?
Ответ:

5.7. Окна опасности появляются не так часто и существуют они недолго. Выберите один ответ:
- Верно
- Неверно

5.8. Угрозу перехвата данных следует учитывать только при начальном конфигурировании элементов ИТ инфраструктуры. Выберите один ответ:
- Верно
- Неверно

5.9. Самыми частыми и самыми опасными угрозами доступности являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих ИТ-инфраструктуру. Выберите один ответ:
- Верно
- Неверно

5.10. Как называется в информационной безопасности выполнение действий под видом лица, обладающего полномочиями для доступа к данным?
Ответ:

6. **Критерии оценивания:** При выполнении тестирования обеспечивается самостоятельность выполнения тестов: из аудитории удаляются посторонние, преподавателем контролируется неиспользование слушателем интернет-источников, учебников и иных пособий, за исключением личного конспекта слушателя (допускается, как рукописный, так и электронный вариант). Тестирование проводится в ЭУМК на базе образовательного портала АлтГУ, за ограниченное время. Оценка выставляется автоматически по окончанию теста или отведённого времени.

7. **Рекомендуемый перечень вопросов для самостоятельной подготовки:**

7.1. Понятие информационной безопасности. Основные составляющие информационной безопасности.

7.2. Основные угрозы информационной безопасности. Основные понятия.

7.3. Наиболее распространённые угрозы доступности.

7.4. Основные угрозы целостности.

7.5. Основные угрозы конфиденциальности.

7.6. Вредоносное программное обеспечение. Основные понятия.

7.7. Классификация вредоносных программ.

7.8. Способы защиты от вредоносных программ.

7.9. Программно-технический уровень информационной безопасности. Основные понятия.

7.10. Особенности современных информационных систем.

7.11. Архитектурная безопасность.

7.12. Управление доступом. Идентификация и аутентификация.

7.13. Авторизация.

7.14. Протоколы AAA.

7.15. Протоколирование и аудит. Основные понятия.

7.16. Активный аудит

7.17. Шифрование. Основные понятия.

7.18. Обеспечение конфиденциальности. Симметричное шифрование.

7.19. Обеспечение конфиденциальности. Асимметричное шифрование.

7.20. Контроль целостности. Электронная цифровая подпись. Цифровые сертификаты.

7.21. Административный уровень информационной безопасности. Основные понятия. Комплексная система защиты информации.

7.22. Политика безопасности.

7.23. Программа безопасности.

7.24. Синхронизация программы безопасности с жизненным циклом ИС.

7.25. Законодательный уровень информационной безопасности. Основные понятия.

7.26. Закон «Об информации, информатизации и защите информации».

7.27. Закон «О лицензировании отдельных видов деятельности».

7.28. Закон «Об участии в международном информационном обмене».

7.29. Закон «Об электронной цифровой подписи».

7.30. Нормативные документы.

ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ

1. **Форма проведения промежуточной аттестации:** экзамен.

2. **Процедура проведения:**

   Для получения экзамена тест (итоговый) является обязательным, однако, в случае выполнения всех лабораторных работ есть возможность получить оценку за курс «автоматом» (оценка вычисляется только с учётом практической работы).

   Тест состоит из 20 вопросов по изученному теоретическому материалу, ограничение по времени: 20 мин, метод оценивания: Последняя попытка. Слушателю разрешено сделать 3 попытки. Слушатель должен ответить на вопросы теста самостоятельно, без использования интернет-источников, учебников и иных пособий, за исключением личного конспекта слушателя. Личный конспект слушателя (допускается, как рукописный, так и электронный вариант) должен быть предъявлен преподавателю (для проверки подлинности авторства) перед проведением тестирования. Тестирование проводится в ЭУМК на образовательном портале АлтГУ. Оценка выставляется автоматически по окончанию теста или отведённого времени.

3. **Проверяемые компетенции (код):** ОПК-3, ОПК-4, ПК-1, ПК-3, ПК-10.

4. **Индикаторы достижения:**

   - ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
   - ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
   - ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
   - ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.
   - ПК-1.2. Уметь проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе.
   - ПК-3.1. Знать методы и технологии проектирования ИС по видам обеспечения.
   - ПК-3.2. Уметь применять методы и технологии проектирования ИС по видам обеспечения.
   - ПК-10.1. Знать виды и способы формирования организационных структур информационной службы; международные стандарты управления автоматизированными информационными системами и информационной службой предприятия.
   - ПК-10.2. Уметь формулировать требования бизнеса и цели внедрения автоматизированной информационной системы; грамотно оценивать затраты, связанные с разработкой, внедрением.

5. **Пример оценочного средства:**

   5.1. Сколько уровней детализации целесообразно для рассмотрения политики безопасности? Выберите один ответ:

   - 4
   - 1
   - 5
   - 3
   - 2
   - 7

   5.2. Укажите виды блочных шифров. Выберите один или несколько ответов:

- Покадровый шифр
- Симметричный шифр
- Потоковый шифр
- Шифры подстановки
- Асимметричный шифр
- Шифры перестановки

5.3. Как называется прокси-сервер, обрабатывающий запросы от любых IP-адресов в Интернете?
Ответ:

5.4. Какой метод активного аудита вызывает наименьшее число ошибок первого рода?
Выберите один ответ:

- метод грубой силы
- статистический метод
- сигнатурный метод
- блочный метод
- потоковый метод

5.5. Как называется алгоритм шифрования, для которого математически доказана его абсолютная криптографическая стойкость?
Ответ:

5.6. Укажите виды нарушения статической целостности.
Выберите один или несколько ответов:

- кража данных
- ввод неверных (фальшивых) данных
- переупорядочение данных
- дублирование данных
- изменение данных

5.7. Как называется потенциальная возможность определённым образом нарушить информационную безопасность?
Ответ:

5.8. Какие меры позволяют значительно повысить надёжность парольной защиты?
Выберите один или несколько ответов:

- ограничение доступа к файлу паролей
- обучение пользователей
- наложение технических ограничений
- шифрование паролей
- шифрование файла с паролями
- управление сроком действия паролей
- использование программных генераторов паролей
- ограничение числа неудачных попыток входа в систему

5.9. К административному уровню информационной безопасности относятся разработка законов и нормативных актов, ориентированные на людей, в области ИБ.
Выберите один ответ:

- Верно
- Неверно

5.10. Один экранирующий сервис может экранировать только один элемент.
Выберите один ответ:

- Верно
- Неверно

5.11. Как называется действие, выполняемое в рамках имеющихся полномочий, но нарушающие политику безопасности?
Выберите один ответ:

- Протоколирование
- Сигнатура атаки
- Активный аудит
- Подозрительная активность
- Злоупотребление полномочиями
- Аудит

5.12. Как называется защита от несанкционированного доступа к информации?
Ответ:

5.13. Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик.
Выберите один ответ:

- Верно
- Неверно

5.14. Кроме удостоверяющего центра, сам пользователь может изменять информацию о себе, без нарушения целостности сертификата.
Выберите один ответ:

- Верно
- Неверно

5.15. Существует единая общепринятая классификация и номенклатура вредоносных программ.
Выберите один ответ:

- Верно
- Неверно

5.16. Многоразовые пароли являются более эффективным средством, чем одноразовые пароли.
Выберите один ответ:

- Верно
- Неверно

5.17. Наиболее распространённой хеш-функцией является MD4.
Выберите один ответ:

- Верно
- Неверно

5.18. Как называется список, который определяет, какие субъекты могут получать доступ к конкретному объекту, и какие именно операции разрешено или запрещено этому субъекту проводить над объектом?
Ответ:

5.19. Частая смена программного и аппаратного обеспечения (с целью увеличения мощностей) ведёт к укреплению информационной безопасности.
Выберите один ответ:

- Верно
- Неверно

5.20. Как называется самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя?
Ответ:

6. Критерии оценивания: Для расчёта итогового балла B применяется следующая формула:

$$B = T_{\text{вход.}} + T_{\text{итог.}} + D + 0{,}7\frac{\sum\limits_{i=1}^{N} w_i l_i}{N} + \sum_{i=1}^{M} a_i, \tag{1}$$

где $T_{\text{итог.}} \leqslant 10$ — балл за итоговый тест; $T_{\text{вход.}} \leqslant 10$ — балл за входной тест; D — балл за прохождение дистанционного курса (при предъявлении сертификата $D = 10$); $l_i \leqslant 100$ — балл

за i-ю выполненную слушателем работу; w_i — вес за i-ю работу (0,5 или 1); N — полное число практических работ в дисциплине; a_i — дополнительный (бонусный) балл, который слушатель может получить за активность (не более, чем 1 балл за одну лекцию); M — количество прочитанных лекций.

Поскольку для промежуточного контроля используется такая форма контроля, как экзамен, по итоговому баллу (в 100-балльной шкале) ставится отметка, в соответствии с табл. 3.

Таблица 3.

Сопоставление шкал оценивания

100-балльная шкала	0–49	50–69	70–89	90–100
4-балльная шкала (уровень освоения)	Неудовлетворительно (уровень не сформирован)	Удовлетворительно (пороговый уровень)	Хорошо (базовый уровень)	Отлично (повышенный уровень)