

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
БУРЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ДОРЖИ БАНАЗАРОВА
ИНСТИТУТ МАТЕМАТИКИ, ФИЗИКИ И КОМПЬЮТЕРНЫХ НАУК
КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ИНФОРМАТИКИ

Утверждена на заседании
Ученого совета ИМФКН
«__»_____ 202__ г.
Протокол № __

Рабочая программа дисциплины
Информационная безопасность

Направление подготовки / специальность
09.04.02 Информационные системы и технологии

Профиль
Проектирование, разработка и эксплуатация информационных систем

Квалификация (степень) выпускника
Магистр

Форма обучения
Очная

Улан-Удэ
2025

Пояснительная записка

Цели освоения дисциплины

формирование у магистрантов комплексного представления о принципах, методах и средствах обеспечения информационной безопасности информационных систем, а также развитие навыков практического применения этих знаний для защиты информации от угроз различного характера.

Задачи дисциплины:

- формирование системных представлений об управлении информационными рисками;
- изучение методов и средств комплексной защиты информации в информационных системах коммерческих предприятий и государственных учреждений;
- формирование практических навыков анализа защищенности информационных систем, использования встроенных возможностей ОС, MS Office, Брандмауэра Windows, Internet Explorer, а также антивирусных и криптографических средств для обеспечения безопасности информации;
- получение теоретических знаний и практических навыков при решении типовых задач по обеспечению информационной безопасности;
- изучение проблем защиты информации, стоящих перед современной вычислительной техникой;
- формирование навыков использования полученных знаний для правильного выбора решений при разработке криптографических, организационных, технических средств защиты информации.

Место дисциплины в структуре образовательной программы

Учебная дисциплина Б1.В.ДВ.02.01 «Информационная безопасность» относится к части, формируемой участниками образовательных отношений Блока 1, является дисциплиной по выбору.

Дисциплина опирается на знания и навыки, полученные студентами при изучении дисциплин "Программирование", "Информационные технологии", "Информационные системы", "Правоведение".

В результате освоения дисциплины студент должен:

Планируемые результаты обучения по дисциплине и индикаторы достижения компетенций.

УК-2. Способен управлять проектом на всех этапах его жизненного цикла

УК-2.1 формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления

УК-2.4 осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта

ПК-1. Способен планировать работы в проектах в области ИТ малого и среднего уровня сложности

ПК-1.1. Назначает и распределяет ресурсы в рамках управления работами по сопровождению и проектами создания (модификации) ИС

Знать:

- понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации;
- стандартные программные средства набора текста и баз данных;
- правовые акты в области защиты государственной тайны и информационной безопасности;
- правовые основы организации защиты государственной тайны и конфиденциальной информации;
- основные понятия информационной безопасности;
- основные принципы организации и алгоритмы функционирования систем безопасности

- в современных операционных системах и оболочках;
- возможности применения в работе современных системных программных средств: операционных систем, операционных оболочек, обслуживающих программ;
 - основные принципы организации и алгоритмы функционирования операционных систем и оболочек;
 - проблемы и направления развития системных программных средств.

Уметь:

- использовать программные и аппаратные средства персонального компьютера;
- ориентироваться в современной системе источников информации;
- использовать современные информационные технологии в своей профессиональной деятельности;
- применять средства антивирусной защиты;
- анализировать информационную безопасность многопользовательских систем;
- пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа;
- видеть и формулировать проблему, видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи.

Владеть:

- методами анализа и оценки рисков информационной безопасности;
- навыками поиска информации в глобальной информационной сети Интернет, работы с базами данных и интернет-ресурсами;
- современной терминологией и методологией в области информационной безопасности;
- навыками применения аппаратных и программных средств обеспечения информационной безопасности;
- навыками противостояния типовым удаленным атакам.

Планируемые результаты освоения образовательной программы:

Объем дисциплины в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 6 зачетные единицы, 216 часа.

№	Название разделов дисциплины	Лабораторная работа	Самостоятельная работа
	Семестр 1	14	58
1	Введение в информационную безопасность	6	30
2	Уровни обеспечения информационной безопасности	8	28
	Семестр 2	12	132
1	Программно-аппаратные средства защиты информации	12	132

Тематическое планирование курса

Темы

Введение в информационную безопасность

Семестр 1

Введение в информационную безопасность

Лабораторная работа. 2(0) ч. 1. Основные понятия: задачи, объект, предмет, методы информационной безопасности. Политика в сфере обеспечения информационной безопасности России. Концептуальная модель информационной безопасности. Официальные органы, обеспечивающие информационную безопасность в Российской Федерации. Составляющие концептуальной модели информационной безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации. Понятие информации. Сведения и данные, отличие от информации. Информация по уровню доступа. Конфиденциальность информации. Понятие конфиденциальной информации. Классификация конфиденциальной информации. Понятие государственной тайны. Степени грифа секретности. Виды сведений составляющих государственную тайну. Перечень информации, не подлежащей к засекречиванию. Классификация видов профессиональной тайны и объекты их приложения.

Лабораторная работа. 2(0) ч. 2. Понятие угроз безопасности. Классификация угроз информационной безопасности. Основная классификация угроз: угрозы нарушения конфиденциальности информации, угрозы нарушения целостности информации, угрозы нарушения доступности информации. Методы перечисления угроз. Случайные и преднамеренные угрозы. Технологические возможности злоумышленников по преодолению систем защиты информации. Признаки угрозы безопасности информации в распределенных вычислительных системах (РВС): по характеру воздействия; по цели воздействия; по условию начала осуществления воздействия; по наличию обратной связи с атакуемым объектом; по расположению субъекта атаки относительно атакуемого объекта; по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие.

Лабораторная работа. 2(0) ч. 3. Разграничение прав пользователей в защищенных версиях операционной системы Windows.

Самостоятельная работа. 10(0) ч. Подготовка сообщения: "История развития информационной безопасности в России".

Самостоятельная работа. 10(0) ч. Анализ конкретных примеров угроз (на основе публикаций в СМИ или отчетов компаний по ИБ).

Самостоятельная работа. 10(0) ч. Подготовить доклад/эссе по темам: "Социальная инженерия как фактор риска информационной безопасности", "Эволюция вредоносного ПО в XXI веке".

Уровни обеспечения информационной безопасности

Семестр 1

Уровни информационной безопасности

Лабораторная работа. 2(0) ч. 4. Уровни защиты информации. Ключевые понятия информационной безопасности - политика безопасности и программа безопасности. Структура соответствующих документов, меры по их разработке и сопровождению. Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня: управление персоналом; физическая защита; поддержание работоспособности; реагирование на нарушения режима безопасности; планирование восстановительных работ.

Лабораторная работа. 2(0) ч. 5. Стандарты и спецификации в области информационной безопасности. Классификация стандартов в области информационной безопасности. «Оранжевая книга», ее структура и группы классов защищенности. Руководящие документы Гостехкомиссии России. Понятие несанкционированного доступа (НСД). Направления защиты от НСД. Основные способы НСД. Принципы защиты от НСД. Классификация нарушителей. Понятие системы разграничения доступа (СРД). Основные функции СРД.

Лабораторная работа. 2(0) ч. 6. Правовое обеспечение информационной безопасности. Обзор российского законодательства в сфере информационных технологий.

Составляющие концептуальной модели информационной безопасности. Современная концепция информационной безопасности.

Лабораторная работа. 2(0) ч. 7. Реализация политики безопасности в защищенных версиях операционной системы Windows.

Самостоятельная работа. 10(0) ч. Изучение нормативно-правовой базы РФ в области ИБ (ФЗ, приказы ФСТЭК, Роскомнадзора).

Самостоятельная работа. 12(0) ч. Подготовка обзора стандартов ISO 27000.

Самостоятельная работа. 6(0) ч. Подготовка сообщения "Влияние нормативно-правового регулирования на развитие IT-индустрии".

Программно-аппаратные средства защиты информации

Семестр 2

Программно-аппаратные средства защиты информации

Лабораторная работа. 2(0) ч. 8. Техническое обеспечение информационной безопасности.

Понятие сервиса безопасности. Понятие архитектурной безопасности. Классификация сервисов безопасности. Средства идентификации и аутентификации пользователей.

Идентификация и аутентификация, управление доступом. Парольная аутентификация.

Одноразовые пароли. Система S/KEY компании Bellcore. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Матрица доступа.

Произвольное (или дискреционное) управление доступом. Принудительное (мандатное) управление доступом. Списки управления доступом. Ограничивающий интерфейс.

Ролевое управление доступом. Статическое разделение обязанностей. Динамическое разделение обязанностей.

Лабораторная работа. 2(0) ч. 9. Аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства аутентификации электронных данных и средства управления ключевой информацией. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование.

Лабораторная работа. 2(0) ч. 10. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.

Лабораторная работа. 2(0) ч. 11. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.

Лабораторная работа. 2(0) ч. 12. Настройка безопасности базы данных.

Лабораторная работа. 2(0) ч. 13. Моделирование инцидента информационной безопасности и разработка плана реагирования.

Самостоятельная работа. 20(0) ч. Исследование сравнение различных методов аутентификации (преимущества и недостатки).

Самостоятельная работа. 20(0) ч. Разработка рекомендаций по созданию надежных паролей.

Самостоятельная работа. 16(0) ч. Подготовка доклада по темам "Биометрическая аутентификация: перспективы и риски", "Роль человеческого фактора в защите паролей".

Самостоятельная работа. 16(0) ч. Сравнительный анализ моделей управления доступом (DAC, MAC, RBAC).

Самостоятельная работа. 22(0) ч. Разработка матрицы доступа для информационной системы организации.

Самостоятельная работа. 16(0) ч. Изучение принципов работы различных типов межсетевых экранов.

Самостоятельная работа. 22(0) ч. Анализ работы системы обнаружения вторжений (IDS) на основе журнала событий.

Семестр	Контрольные точки	Баллы
1	Текущий контроль в разделе «Введение в информационную безопасность»	
	Доклад, сообщение	10
	Тест	5
	Выполнение и оформление отчетности по лабораторной работе	15
1	Текущий контроль в разделе «Уровни обеспечения информационной безопасности»	
	Тест	5
	Выполнение и оформление отчетности по лабораторной работе	20
	Доклад, сообщение	5
1	Зачет	
	зачет	40
Итого за семестр 1:		100
2	Текущий контроль в разделе «Программно-аппаратные средства защиты информации»	
	Тест	5
	Выполнение и оформление отчетности по лабораторной работе	30
	Доклад, сообщение	25
2	Зачет	
	зачет	40
Итого за семестр 2:		100

Учебно-методическое и информационное обеспечение учебного процесса

Образовательные технологии (в том числе на занятиях, проводимых в интерактивных формах).

Рекомендуемые образовательные технологии: лекции, практические занятия, самостоятельная работа студентов.

При проведении занятий рекомендуется использование активных и интерактивных форм занятий (компьютерных симуляций, деловых и ролевых игр, проектных методик,

мозгового штурма, разбора конкретных ситуаций, коммуникативного эксперимента, коммуникативного тренинга, иных форм) в сочетании с внеаудиторной работой. Удельный вес занятий, проводимых в интерактивных формах, должен составлять не менее 30 % аудиторных занятий.

Учебно-методические материалы, в том числе методические указания для обучающихся по освоению дисциплины

Теоретическая часть курса, общие вопросы методики и технологий применения компьютерных средств излагаются преподавателем в лекционном курсе. Отдельные вопросы могут выноситься на самостоятельное изучение. Студент должен иметь в виду, что на лекциях преподаватель определяет такие вопросы и рекомендует необходимую для их изучения литературу, источники и др. ресурсы. Для успешного освоения курса необходимо внимательно фиксировать основные положения лекции, своевременно их усваивать, при необходимости самостоятельно прорабатывать, используя основную и дополнительную литературу.

Для приобретения навыков общения с ПК в процессе освоения инструментальных систем и отладки программ предназначены лабораторные занятия. Лабораторные занятия проводятся в специальных классах, оборудованных средствами вычислительной техники.

На первом лабораторном занятии студенты получают инструктаж по технике безопасности при работе в классе и знакомятся с особенностями работы на конкретной вычислительной машине. Последующие лабораторные работы заключаются в освоении инструментальных систем и отладке программ решения типовых задач. Индивидуальные задания и методические указания к выполнению каждой последующей лабораторной работы студент получает, как правило, на предыдущем занятии. Подготовка к выполнению лабораторных работ осуществляется в часы самостоятельной работы.

Студенты, не подготовившиеся к занятиям, к работе на компьютере не допускаются.

По каждой выполненной лабораторной работе студент оформляет отчет по установленной форме.

Самостоятельные занятия под контролем преподавателя предназначены для самостоятельного изучения студентами тех разделов курса, по которым не предусмотрено чтение лекций, либо проводятся лекции обзорного характера. По усмотрению преподавателя в часы индивидуальных занятий студентам может поручаться выполнение других заданий.

Занятия проводятся с академической группой или с половиной группы в часы, установленные расписанием занятий. На занятиях студент должен иметь конспект лекций, учебную и справочную литературу, отдельную тетрадь для записей. Весь теоретический материал, изученный в процессе индивидуальных занятий, должен быть законспектирован.

Оценочные средства

По данной дисциплине разработаны оценочные средства, критерии их оценивания, а также методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

- [ФОС_инф_без_магистр.doc](#)

Список литературы

Перечень основной и дополнительной литературы, необходимой для освоения дисциплины.

Основная

1. [Информационная безопасность](#): Учебное пособие для вузов/Суворова Г. М.. — Москва: Юрайт, 2022. — 253 с.
Режим доступа: <https://urait.ru/bcode/496741>
2. [Информационная безопасность и защита информации](#): Учебное пособие для вузов/Зенков А. В.. — Москва: Юрайт, 2021. — 104 с.
Режим доступа: <https://urait.ru/bcode/477968>
3. [Защита информации](#): Учебное пособие для вузов/Внуков А. А.. — Москва: Юрайт, 2022. — 161 с.
Режим доступа: <https://urait.ru/bcode/490277>
4. [Защита информации: основы теории](#): Учебник для вузов/Щеглов А. Ю., Щеглов К. А.. — Москва: Юрайт, 2022. — 309 с.
Режим доступа: <https://urait.ru/bcode/490019>

Дополнительная

1. [Информационная безопасность: защита и нападение](#)/А. А. Бирюков. — Москва: ДМК Пресс, 2012. — 474 с.
Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=39990
2. Цыбикова Т. С. Информационная безопасность: курс лекций : [учеб. пособие : для студентов специальности "Прикладная информатика в экономике"]/Т. С. Цыбикова; М-во сел. хоз. РФ, Департамент науч.-технол. политики и образования, ФГОУ ВПО "Бурят. гос. с.-х. акад. им. В. Р. Филиппова". — Улан-Удэ: Изд-во БГСХА им. В. Р. Филиппова, 2010. — 237 с.
3. [Защита информации в компьютерных системах и сетях](#)/Шаньгин В.Ф.. — Москва: ДМК Пресс, 2012
Режим доступа: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=3032
4. [Защита информации: криптоалгоритмы хеширования](#): учебное пособие для вузов/Игнатъев Е. Б.. — Санкт-Петербург: Лань, 2023. — 264 с.
Режим доступа: <https://e.lanbook.com/book/311792>
5. [Защита информации в банковских системах](#): Учебное пособие для вузов/Внуков А. А.. — Москва: Юрайт, 2022. — 246 с.
Режим доступа: <https://urait.ru/bcode/490278>

Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Федеральный портал. Российское образование. <http://www.edu.ru/>
2. Российский образовательный портал. <http://www.school.edu.ru/default.asp>
3. Федеральный правовой портал. Юридическая Россия. <http://www.law.edu.ru/>
4. Информационно-коммуникационные технологии в образовании. <http://www.ict.edu.ru/>
5. Российский портал открытого образования. <http://www.openet.edu.ru/>
6. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: <http://cyberrus.com/>
7. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/>

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

1. Личный кабинет преподавателя или студента БГУ <http://my.bsu.ru/>
2. Портал электронного обучения БГУ
3. Office Standard 2007
4. Windows 7 Корпоративная

5. Free Pascal

6. Microsoft Visual Studio 2019

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. Аудитория для проведения учебных занятий всех типов - 0419.

2. Компьютер - 13 шт.

3. Проектор - 1 шт.

4. Интерактивная доска - 1 шт.

4. Доска аудиторная настенная - 1 шт.

5. Комплект учебной мебели на 13 посадочных мест.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «БУРЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ ДОРЖИ БАНЗАРОВА»
Институт математики, физики и компьютерных наук
Кафедра вычислительной техники и информатики

**Фонд оценочных средств по дисциплине
Информационная безопасность**

Направление подготовки/ специальность

09.04.02– Информационные системы и технологии

Профиль подготовки /специализация

Проектирование, разработка и эксплуатация информационных систем

Квалификация (степень) выпускника

Магистр

Форма обучения

очная

Улан-Удэ
2025

Паспорт

фонда оценочных средств

по учебной дисциплине «Информационная безопасность»

09.04.02 – Информационные системы и технологии

№	Контролируемые разделы, темы, модули	Наименование компетенции	Этапы формирования	Оценочные средства	
				Вид	Количество
1	Введение в информационную безопасность	УК-2.1 УК-2.4 ПК-1.1	1 семестр	Доклад Тест Лабораторная работа	12 20 1
2	Уровни обеспечения информационной безопасности	УК-2.1 УК-2.4 ПК-1.1	1 семестр	Тест Лабораторная работа	20 1
3	Программно-аппаратные средства защиты информации	УК-2.1 УК-2.4 ПК-1.1	2 семестр	Тест Лабораторная работа	20 2
4	Методы криптографической защиты информации	УК-2.1 УК-2.4 ПК-1.1	2 семестр	Тест Лабораторная работа	20 3

¹Наименования разделов, тем, модулей соответствуют рабочей программе дисциплины.

УК-2.1 – формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления.

УК-2.4 – осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта.

ПК – 1.1 – назначает и распределяет ресурсы в рамках управления работами по сопровождению и проектами создания (модификации) ИС.

Вопросы к зачету

Раздел 1. Введение в информационную безопасность).

1. Понятие информационной безопасности.
2. Основные понятия; Политика безопасности; Программа безопасности.
3. Основные составляющие информационной безопасности; Важность и сложность проблемы.
4. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.
5. Важность законодательного уровня информационной безопасности.
6. Обзор российского законодательства в области информационной безопасности.
7. Административный уровень информационной безопасности.
8. Основные понятия программно-технического уровня информационной безопасности.
9. Особенности современных информационных систем, существенные с точки зрения безопасности.

Раздел 2. Уровни обеспечения информационной безопасности.

10. Основные определения и критерии классификации угроз.
11. Вредоносное программное обеспечение.
12. Основные классы мер процедурного уровня информационной безопасности.
13. Управление персоналом. Физическая защита. Поддержание работоспособности.
14. Синхронизация программы безопасности с жизненным циклом систем
15. Этапы управления рисками.
16. Реагирование на нарушения режима безопасности; Планирование восстановительных работ.

Раздел 3. Программно-аппаратные средства защиты информации.

17. Основные понятия идентификации и аутентификации.
18. Основные понятия управления доступом.
19. Моделирование и аудит, шифрование, контроль целостности.
20. Протоколирование и аудит.
21. Классификация межсетевых экранов. Анализ защищенности.
22. Основы мер обеспечения высокой доступности.
23. Программное обеспечение обслуживаемости.
24. Туннелирование и управление – основные понятия.

Раздел 4. Методы криптографической защиты информации.

25. Основные понятия криптологии.
26. Методы криптографического преобразования данных.
27. Симметричные и асимметричные криптосистемы.
28. Криптографическая система DES и ее модификации.
29. Криптографическая система ГОСТ 28147-89.
30. Электронная цифровая подпись и ее применение.

Оценивание ответа при собеседовании – максимальный балл - 40:

Баллы для учета в рейтинге (оценка ответа на зачете)	Степень удовлетворения критериям
34-40 баллов «отлично»	В ответе качественно раскрыто содержание темы. Ответ хорошо структурирован. Прекрасно освоен понятийный аппарат. Продemonстрирован высокий уровень понимания материала. Превосходное умение формулировать свои мысли, обсуждать

	дискуссионные положения.
27-33 баллов «хорошо»	Основные вопросы темы раскрыты. Структура ответа в целом адекватна теме. Хорошо освоен понятийный аппарат. Продемонстрирован хороший уровень понимания материала. Хорошее умение формулировать свои мысли, обсуждать дискуссионные положения.
20-26 баллов «удовлетворительно»	Тема частично раскрыта. Ответ слабо структурирован. Понятийный аппарат освоен частично. Понимание отдельных положений из материала по теме. Удовлетворительное умение формулировать свои мысли, обсуждать дискуссионные положения.
19 баллов и меньше «неудовлетворительно»	Тема не раскрыта. Понятийный аппарат освоен неудовлетворительно. Понимание материала фрагментарное или отсутствует. Неумение формулировать свои мысли, обсуждать дискуссионные положения.

Шкала перевода в баллы:

Оценка	Общий балл
34-40	5 (отлично)/зачтено
27-33	4 (хорошо)/зачтено
20-26	3 (удовлетворительно)/зачтено
Менее 20 баллов	2 (неудовлетворительно)/не зачтено

Составитель: к.п.н., доцент кафедры ВТИ _____ Т.С. Цыбикова

Примерные темы для докладов, сообщений

1. Свойства информации как объекта защиты
2. Основной закон Российской Федерации. Международные стандарты в области информационной безопасности и защиты информации
3. Модели угроз и модели нарушителей информационных систем. Дестабилизирующие факторы.
4. Модели угроз согласно нормативным документам ФСТЭК России.
5. Электронные ключи, электронные замки. Средства для оценки защищенности
6. Стандарты шифрования ГОСТ 28147-89, DES, AES, RSA, PGP. Стандарты электронно-цифровой подписи ГОСТ 34.10-04, ГОСТ 34.10-2001, DSS
7. Электронные платежи. Электронный кошелек
8. Средства идентификации. Биометрическая идентификация
9. Удостоверяющий центр. Использование сертификатов ЭЦП для работы в сети. Использование SSL, TLS.
10. Неправомерный доступ к компьютерной информации.
11. Способы совершения преступления в сфере компьютерной информации.
12. Преступления в сфере компьютерной информации.

Оценивание доклада/сообщения – максимальный балл - 5:

Баллы для учета в рейтинге (оценка ответа на зачете)	Степень удовлетворения критериям
5 баллов	обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы
4 балла «хорошо»	основные требования к докладу и его защите выполнены, но при этом допущены недочёты имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы
3 балла «удовлетворительно»	имеются существенные отступления от требований к докладу. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании докладаа или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.
2 балла	тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Примерные тестовые задания

Раздел 1: Введение в информационную безопасность

1. Защита информации от утечки - это деятельность по предотвращению:
 - а) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
 - б) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
 - в) воздействия на защищаемую информацию ошибок пользователя информацией, сбоев технических и программных средств информационных систем, а также природных явлений;
 - г) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
 - д) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
2. Защита информации это:
 - а) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
 - б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
 - в) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
 - г) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
 - д) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
3. Естественные угрозы безопасности информации вызваны:
 - а) деятельностью человека;
 - б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
 - в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
 - г) корыстными устремлениями злоумышленников;
 - д) ошибками при действиях персонала.
4. Искусственные угрозы безопасности информации вызваны:
 - а) деятельностью человека;
 - б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
 - в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
 - г) корыстными устремлениями злоумышленников;
 - д) ошибками при действиях персонала.
5. К основным непреднамеренным искусственным угрозам АСОИ относится:
 - а) физическое разрушение системы путем взрыва, поджога и т.п.;
 - б) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
 - в) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
 - г) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

- д) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.
6. К посторонним лицам нарушителям информационной безопасности относится:
- а) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
 - б) персонал, обслуживающий технические средства;
 - в) технический персонал, обслуживающий здание;
 - г) пользователи;
 - д) сотрудники службы безопасности.
 - е) представители конкурирующих организаций.
 - ж) лица, нарушившие пропускной режим;
7. К внутренним нарушителям информационной безопасности относится:
- а) клиенты;
 - б) пользователи системы;
 - в) посетители;
 - г) любые лица, находящиеся внутри контролируемой территории;
 - д) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
 - е) персонал, обслуживающий технические средства.
 - ж) сотрудники отделов разработки и сопровождения ПО;
 - з) технический персонал, обслуживающий здание
8. Информация это -
- а) сведения, поступающие от СМИ
 - б) только документированные сведения о лицах, предметах, фактах, событиях
 - в) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
 - г) только сведения, содержащиеся в электронных базах данных
9. Информация
- а) не исчезает при потреблении
 - б) становится доступной, если она содержится на материальном носителе
 - в) подвергается только "моральному износу"
 - г) характеризуется всеми перечисленными свойствами
10. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
- а) достоверной
 - б) конфиденциальной
 - в) документированной
 - г) коммерческой тайной
11. Формы защиты интеллектуальной собственности -
- а) авторское, патентное право и коммерческая тайна
 - б) интеллектуальное право и смежные права
 - в) коммерческая и государственная тайна
 - г) гражданское и административное право
12. По принадлежности информационные ресурсы подразделяются на
- а) государственные, коммерческие и личные
 - б) государственные, не государственные и информацию о гражданах
 - в) информацию юридических и физических лиц
 - г) официальные, гражданские и коммерческие
13. К негосударственным относятся информационные ресурсы
- а) созданные, приобретенные за счет негосударственных учреждений и организаций
 - б) созданные, приобретенные за счет негосударственных предприятий и физических лиц

- в) полученные в результате дарения юридическими или физическими лицами
 - г) все указанные
14. По доступности информация классифицируется на
- а) открытую информацию и государственную тайну
 - б) конфиденциальную информацию и информацию свободного доступа
 - в) информацию с ограниченным доступом и общедоступную информацию
 - г) виды информации, указанные во всех пунктах
15. К конфиденциальной информации относятся документы, содержащие
- а) государственную тайну
 - б) законодательные акты
 - в) "ноу-хау"
 - г) сведения о золотом запасе страны
16. Запрещено относить к информации ограниченного доступа
- а) информацию о чрезвычайных ситуациях
 - б) информацию о деятельности органов государственной власти
 - в) документы открытых архивов и библиотек
 - г) все, перечисленное
17. К конфиденциальной информации не относится
- а) коммерческая тайна
 - б) персональные данные о гражданах
 - в) государственная тайна
 - г) "ноу-хау"
18. Если информация искажена умышленно, то это называют
- а) дезинформацией
 - б) потерей ценности
 - в) нарушением конфиденциальности
 - г) нарушением целостности
19. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена
- а) конфиденциальность
 - б) целостность
 - в) аутентичность
 - г) апеллируемость
 - д) надежность
 - е) точность
20. Процедура проверки подлинности, позволяющая достоверно убедиться, что пользователь является именно тем, кем он себя объявляет:
- а) санкционированный доступ
 - б) несанкционированный доступ
 - в) идентификация
 - г) аутентификация
 - д) нет правильных вариантов

Раздел 2: Уровни обеспечения информационной безопасности

1. В число целей политики безопасности верхнего уровня входят:
- а) решение сформировать или пересмотреть комплексную программу безопасности;
 - б) обеспечение базы для соблюдения законов и правил;
 - в) обеспечение конфиденциальности почтовых сообщений.
2. В число целей политики безопасности верхнего уровня входят:
- а) управление рисками;
 - б) определение ответственных за информационные сервисы;

- в) определение мер наказания за нарушения политики безопасности.
- 3. В рамках политики безопасности нижнего уровня осуществляются:
 - а) стратегическое планирование;
 - б) повседневное администрирование;
 - в) отслеживание слабых мест защиты.
- 4. Политика безопасности строится на основе:
 - а) общих представлений об ИС организации;
 - б) изучения политик родственных организаций;
 - в) анализа рисков.
- 5. В число целей политики безопасности верхнего уровня входят:
 - а) формулировка административных решений по важнейшим аспектам реализации программы безопасности;
 - б) выбор методов аутентификации пользователей;
 - в) обеспечение базы для соблюдения законов и правил.
- 6. Риск является функцией:
 - а) размера возможного ущерба;
 - б) числа пользователей информационной системы;
 - в) уставного капитала организации.
- 7. В число этапов управления рисками входят:
 - а) идентификация активов;
 - б) ликвидация пассивов;
 - в) выбор объектов оценки.
- 8. Первый шаг в анализе угроз — это:
 - а) идентификация угроз;
 - б) аутентификация угроз;
 - в) ликвидация угроз.
- 9. Управление рисками включает в себя следующие виды деятельности:
 - а) определение ответственных за анализ рисков;
 - б) оценка рисков;
 - в) выбор эффективных защитных средств.
- 10. Оценка рисков позволяет ответить на следующие вопросы:
 - а) чем рискует организация, используя информационную систему?
 - б) чем рискуют пользователи информационной системы?
 - в) чем рискуют системные администраторы?
- 11. Вопросы информационного обмена регулируются (...) правом
 - а) гражданским
 - б) информационным
 - в) конституционным
 - г) уголовным
- 12. Согласно ст.132 ГК РФ интеллектуальная собственность - это
 - а) исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности
 - б) информация, полученная в результате интеллектуальной деятельности индивида
 - в) литературные, художественные и научные произведения
 - г) изобретения, открытия, промышленные образцы и товарные знаки
- 13. Интеллектуальная собственность включает права, относящиеся к {
 - а) всему, указанному
 - б) литературным, художественным и научным произведениям, изобретениям и открытиям
 - в) исполнительской деятельности артиста, звукозаписи, радио- и телепередачам
 - г) промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям

14. Конфиденциальная информация это {
- а) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ
 - б) сведения, составляющие государственную тайну
 - в) сведения о состоянии здоровья высших должностных лиц
 - г) данные о состоянии преступности в стране
15. Какая информация подлежит защите? {
- а) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу
 - б) информация, циркулирующая в системах и сетях связи
 - в) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
 - г) только информация, составляющая государственные информационные ресурсы
16. Система защиты государственных секретов определяется Законом {
- а) "О государственной тайне"
 - б) "Об информации, информатизации и защите информации"
 - в) "Об органах ФСБ"
 - г) "О безопасности"
17. Государственные информационные ресурсы не могут принадлежать {
- а) всем перечисленным субъектам
 - б) физическим лицам
 - в) коммерческим предприятиям
 - г) негосударственным учреждениям
18. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает {
- а) Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне"
 - б) ГК РФ
 - в) Закон "Об информации, информатизации и защите информации"
 - г) Конституция
19. Классификация и виды информационных ресурсов определены {
- а) Законом "Об информации, информатизации и защите информации"
 - б) Гражданским кодексом
 - в) Конституцией
 - г) всеми перечисленными документами
20. Определение понятия "конфиденциальная информация" дано в {
- а) Законе "Об информации, информатизации и защите информации"
 - б) ГК РФ
 - в) Законе "О государственной тайне"
 - г) УК РФ

Раздел 3: Программно-аппаратные средства защиты информации

1. Активный перехват информации - это перехват, который:
- а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
 - б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
 - в) неправомерно использует технологические отходы информационного процесса;
 - г) осуществляется путем использования оптической техники;
 - д) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

2. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
 - а) активный перехват;
 - б) пассивный перехват;
 - в) аудиоперехват;
 - г) видеоперехват;
 - д) просмотр мусора.
3. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
 - а) активный перехват;
 - б) пассивный перехват;
 - в) аудиоперехват;
 - г) видеоперехват;
 - д) просмотр мусора.
4. Перехват, который осуществляется путем использования оптической техники называется:
 - а) активный перехват;
 - б) пассивный перехват;
 - в) аудиоперехват;
 - г) видеоперехват;
 - д) просмотр мусора.
5. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек:
 - а) целостность
 - б) конфиденциальность
 - в) апеллируемость
 - г) структурность
 - д) точность
 - е) надежность
6. К межсетевым экранам относятся:
 - а) TCP/IP
 - б) DNS
 - в) DES
 - г) RSA
 - д) FireWall
 - е) ГОСТ 34.10
7. Защита локальной сети от несанкционированного доступа со стороны внешней сети осуществляется с помощью:
 - а) шифрования
 - б) аутентификации
 - в) межсетевых экранов
 - г) разграничения доступа в защищаемую сеть из внешней сети и из внутренней сети во внешнюю
 - д) хаба
 - е) маршрутизатора
8. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (COB)
 - а) МЭ были разработаны для активного или пассивного обнаружения, а COB – для активной или пассивной защиты
 - б) МЭ были разработаны для активной или пассивной защиты, а COB – для активного или пассивного обнаружения
 - в) МЭ работают только на сетевом уровне, а COB – еще и на физическом

9. Под угрозой удаленного администрирования в компьютерной сети понимается угроза
 - а) вмешательства в личную жизнь
 - б) перехвата или подмены данных на путях транспортировки
 - в) поставки неприемлемого содержания
 - г) внедрения агрессивного программного кода в рамках активных объектов Web-страниц
 - д) несанкционированного управления удаленным компьютером
10. Методы повышения достоверности входных данных
 - а) Замена процесса ввода значения процессом выбора значения из предлагаемого множества
 - б) Отказ от использования данных
 - в) Многократный ввод данных и сличение введенных значений
 - г) Проведение комплекса регламентных работ
 - д) Использование вместо ввода значения его считывание с машиночитаемого носителя
 - е) Введение избыточности в документ первоисточник
11. Средства защиты объектов файловой системы основаны на...
 - а) задании атрибутов файлов и каталогов, независимых от прав пользователей
 - б) определении прав пользователя на операции с файлами и каталогами
12. Наиболее эффективное средство для защиты от сетевых атак
 - а) использование сетевых экранов или «firewall»
 - б) использование только сертифицированных программ-броузеров при доступе к сети Интернет
 - в) использование антивирусных программ
 - г) посещение только «надёжных» Интернет-узлов
13. Сервисы безопасности:
 - а) контроль целостности
 - б) кэширование записей
 - в) экранирование
 - г) обеспечение безопасного восстановления
 - д) инверсия паролей
 - е) регулирование конфликтов
 - ж) идентификация и аутентификация
 - з) шифрование
14. Для внедрения бомб чаще всего используются ошибки типа:
 - а) отсутствие проверок кодов возврата;
 - б) переполнение буфера;
 - в) нарушение целостности транзакций.
15. Окно опасности появляется, когда:
 - а) становится известно о средствах использования уязвимости;
 - б) появляется возможность использовать уязвимость;
 - в) устанавливается новое ПО.
16. Демилитаризованная зона располагается:
 - а) перед внешним межсетевым экраном;
 - б) между межсетевыми экранами;
 - в) за внутренним межсетевым экраном.
17. Экранирование на сетевом и транспортном уровнях может обеспечить:
 - а) разграничение доступа по сетевым адресам;
 - б) выборочное выполнение команд прикладного протокола;
 - в) контроль объема данных, переданных по ТСР-соединению.
18. Системы анализа защищенности помогают предотвратить:
 - а) известные атаки;

- б) новые виды атак;
 - в) нетипичное поведение пользователей.
19. Среднее время наработки на отказ:
- а) пропорционально интенсивности отказов;
 - б) обратно пропорционально интенсивности отказов;
 - в) не зависит от интенсивности отказов.
20. Туннелирование может использоваться на следующем уровне эталонной семиуровневой модели OSI:
- а) сетевом;
 - б) сеансовом;
 - в) уровне представления.

Раздел 4: Методы криптографической защиты информации

1. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:
- а) гаммирования
 - б) подстановки
 - в) кодирования
 - г) перестановки
 - д) аналитических преобразований
2. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:
- а) гаммирования
 - б) подстановки
 - в) кодирования
 - г) перестановки
 - д) аналитических преобразований
3. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
- а) гаммирования
 - б) подстановки
 - в) кодирования
 - г) перестановки
 - д) аналитических преобразований
4. Что такое RSA?
- а) шифр Rich Standard Advanced
 - б) шифр Rich Standard Algorithm
 - в) шифр Right Security Algorithm
 - г) шифр, названный по именам его создателей: Rivest, Shamir, Adleman
 - д) шифр Rich Size Algorithm
 - е) Real Signature Algorithm
5. Наука о способах двустороннего преобразования информации с целью
- а) конфиденциальной передачи ее по незащищенному каналу
 - б) криптология
 - в) криптография
 - г) стеганография
 - д) криптоанализ
6. Асимметричная криптография подразумевает:
- а) использование одного и того же ключа как для зашифрования, так и для расшифрования
 - б) использование одного (открытого) ключа для зашифрования, второго (секретного) для расшифрования

- в) использование одного (секретного) ключа для зашифрования, второго (открытого) для расшифрования
 - г) использование механических и химических способов сокрытия информации
 - д) сокрытие самого факта передачи информации
7. Криптоанализ - это:
- а) зашифрование сообщения секретным ключом
 - б) расшифрование сообщения по известному ключу
 - в) взлом криптоалгоритмов
 - г) проверка работоспособности вновь разработанных криптоалгоритмов
8. Разделы современной криптографии:
- а) Управление ключами
 - б) Системы электронной подписи
 - в) Симметричные криптосистемы
 - г) Управление паролями
 - д) Управление передачей данных
 - е) Криптосистемы с открытым ключом
 - ж) Криптосистемы с дублированием защиты
9. Что не является задачей криптосистемы?
- а) обеспечение конфиденциальности
 - б) обеспечение целостности данных
 - в) аутентификация данных и их источников
 - г) межсетевое экранирование
10. Что из перечисленного не является функцией управления криптографическими ключами?
- а) генерация
 - б) хранение
 - в) распределение
 - г) изучение
11. Что из перечисленного не относится к разграничению доступа пользователей?
- а) матрицы установления полномочий
 - б) парольное разграничение доступа
 - в) разграничение криптографических ключей
 - г) разграничение доступа по спискам
12. Что из перечисленного не входит в криптосистему?
- а) алгоритм шифрования
 - б) набор ключей, используемых для шифрования
 - в) полиморфик-генератор
 - г) система управления ключами
13. Что не является задачей криптосистемы?
- а) обеспечение конфиденциальности
 - б) регистрация и аудит нарушений
 - в) обеспечение целостности данных
 - г) аутентификация данных и их источников
14. Что является целью криптоанализа?
- а) Определение стойкости алгоритма
 - б) Увеличение количества функций замещения в криптографическом алгоритме
 - в) Уменьшение количества функций подстановки в криптографическом алгоритме
 - г) Определение использованных перестановок
15. Частота применения брутфорс-атак возросла, поскольку:
- а) Возросло используемое в алгоритмах количество перестановок и замещений
 - б) Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам

- в) Мощность и скорость работы процессоров возросла
 - г) Длина ключа со временем уменьшилась
16. При симметричном шифровании для шифрования и расшифровки используются:
- а) два ключа разной длины
 - б) два разных по значению ключа
 - в) один и тот же ключ
 - г) два открытых ключа
17. В чем преимущество RSA над DSA?
- а) Он может обеспечить функциональность цифровой подписи и шифрования
 - б) Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
 - в) Это блочный шифр и он лучше поточного
 - г) Он использует одноразовые шифровальные блокноты
18. Какова эффективная длина ключа в DES?
- а) 56
 - б) 64
 - в) 32
 - г) 16
19. При асимметричном шифровании для шифрования и расшифровки используются:
- а) два взаимосвязанных ключа
 - б) один открытый ключ
 - в) один закрытый ключ
 - г) два открытых ключа
20. Подберите словосочетание к данному определению: _____ - представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом.
- а) закрытый ключ шифрования
 - б) электронная цифровая подпись
 - в) вирусная маска
 - г) открытый ключ шифрования

Оценивание тестовых заданий – максимальный балл - 5:

Баллы для учета в рейтинге	Степень удовлетворения критериям
5 баллов	количество правильных ответов >89%
4 балла	количество правильных ответов 76..89%
3 балла	количество правильных ответов 51..75%
2 балла	количество правильных ответов 25..50%
1 балл	количество правильных ответов 10..24%

Перечень лабораторных работ

1. Разграничение прав пользователей в защищенных версиях операционной системы Windows.
2. Реализация политики безопасности в защищенных версиях операционной системы Windows.
3. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.
4. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.
5. Исследование алгоритма шифрования DES.
6. Исследование алгоритма шифрования RSA.
7. Исследование алгоритма шифрования Эль-Гамала. Исследование электронных цифровых подписей.

Правила выполнения и защиты лабораторных работ

Лабораторные занятия проводятся в компьютерном классе. Каждая работа засчитывается при удовлетворении всем требованиям протокола оценки и может быть оценена в зависимости от срока защиты. Для допуска к зачету должны быть сданы все работы.

Отчет состоит из следующих разделов:

1. Титульный лист

На титульном указываем название образовательного учреждения, кафедры, работы, ФИО студента (по всем правилам оформления титульного листа работ).

2. Введение

Во введении указываются цели работы (из описания заданий в лабораторных работах) и используемые ОС.

3. Постановка задачи

Формулируется постановка задачи своего варианта задания, где даются задания для выполнения.

4. Выполнение заданий

Приводятся результаты выполнения заданий своего варианта. Графический материал оформляется в соответствии с ГОСТ.

5. Выводы

Приводятся выводы по выполненной работе.

Работы, несоответствующие вышеперечисленным требованиям к защите не допускаются.

Оценивание лабораторных работ – максимальный балл – 5 (1 лабораторная работа):

Баллы для учета в рейтинге	Степень удовлетворения критериям
5 баллов	правильные ответы на вопросы + правильно оформленный отчет
4 балла	неполные ответы на вопросы + правильно оформленный отчет
3 балла	правильный или неполный ответ на два вопроса + правильно оформленный отчет
2 балла	правильный или неполный ответ на один вопрос + правильно оформленный отчет
1 балл	правильно оформленный отчет, нет ответов на вопросы

Снижение баллов:

Минус 0,3 балл за:

- отсутствие правильно оформленного отчета по работе на момент начала работы;

- отсутствие выполненной работы (заполненный отчет, собранные схемы) к концу пары;
- отсутствие на паре без уважительной причины (без предупреждения преподавателя) минимум за 24 ч до начала пары;

Минус 0.2 балла за:

- каждую дополнительную попытку защиты;
- опоздание более чем на 15 мин;
- защиту работы позднее второго занятия после ее выполнения.

Примечание: при наборе \leq «2» балла студент не может получить оценку за работу выше «3». В этом случае для получения оценки «3» необходимо защитить работу на «5», иначе оценка «неуд».

Если вы НЕ отвечаете на поставленные вопросы, другой вопрос попросить «чтобы еще разок попробовать» СЕГОДНЯ НЕЛЬЗЯ.

Защита проделанных работ осуществляется в порядке их возрастания. При неудачной попытке защитить работу № N, «попробовать» защитить работу N+1 нельзя.