Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

Институт информационных технологий и радиоэлектроники

Кафедра информатики и защиты информации

Основание: решение кафедры ИЗИ
от « 28 » 12 2016 года.

Зав. кафедрой ИЗИ _____ М.Ю. Монахов

Фонд оценочных средств
для текущего контроля и промежуточной аттестации
при изучении учебной дисциплины
«Технологии обеспечения информационной безопасности»

Направление подготовки: 10.04.01 «информационная безопасность»

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Владимир, 2016

1. Паспорт фонда оценочных средств

Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации при изучении учебной дисциплины «Технологии обеспечения информационной безопасности» разработан в соответствие с рабочей программой, входящей в ОПОП направления подготовки 10.04.01 «информационная безопасность».

№ п/п	Контролируемые разделы (темы) дисциплины	Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Введение. Основные технические сервисы защиты информации в компьютерных системах.	1	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
2	"Слабые" протоколы аутентификации Парольная аутентификация	1	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
3	Двухфакторная аутентификация PIN-коды и одноразовые пароли.	1	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
4	"Сильные" протоколы аутентификации Протоколы типа "запрос-ответ".	1	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
5	Протоколы аутентификации с нулевым разглашением.	1	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
6	Модели контроля доступа в компьютерных системах. Общие сведения о задаче КД.	1	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
7	Дискреционное управление доступом.	1	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
8	Мандатное управление доступом.	1	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
9	Ролевое разграничение доступа. Модель администрирования РРД, дискреционная и мандатная модели	1	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
10	Построение проекта архитектуры сервиса хранения файлов в защищенном исполнении.	2	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
11	Разработка технического задания на сервис хранения файлов в защищенном исполнении.	2	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
12	Реализация каркаса приложений клиента и сервера для хранения файлов.	2	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
13	Разработка протокола обмена сообщениями между клиентом и сервером.	2	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
14	Реализация модуля шифрования содержимого базы данных.	2	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
15	Реализация модели контроля доступа.	2	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
16	Реализация модуля аутентификации	2	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
17	Реализация административных процедур для сервиса хранения файлов в защищенном исполнении	2	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания
18	Тестирование сервиса хранения файлов в защищенном исполнении	2	ПК-1, ПК-2, ПК-3	Контрольные вопросы и задания

Комплект оценочных средств по дисциплине «Технологии обеспечения информационной безопасности» предназначен для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям образовательной программы, в том числе рабочей программы дисциплины «Технологии обеспечения информационной безопасности», для оценивания результатов обучения: знаний, умений, навыков и уровня приобретенных компетенций.

Комплект оценочных средств по дисциплине «Технологии обеспечения информационной безопасности» включает:

1 семестр

1. Оценочные средства для проведения текущего контроля успеваемости:

- комплект вопросов рейтинг-контроля, позволяющих оценивать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, распознавание объектов изучения в рамках определенного раздела дисциплины;

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении заданий по СРС, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

2. Оценочные средства для проведения промежуточной аттестации в форме: контрольные вопросы для проведения зачета, позволяющие провести процедуру измерения уровня знаний и умений обучающихся.

2 семестр

1. Оценочные средства для проведения текущего контроля успеваемости:

- комплект вопросов рейтинг-контроля, позволяющих оценивать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, распознавание объектов изучения в рамках определенного раздела дисциплины;

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

2. Оценочные средства для проведения промежуточной аттестации в форме: контрольные вопросы для проведения экзамена, позволяющие провести процедуру измерения уровня знаний и умений обучающихся.

2. Перечень компетенций, формируемых в процессе изучения дисциплины «Технологии обеспечения информационной безопасности» при освоении образовательной программы по направлению подготовки 10.04.01 «информационная безопасность»

Перечень компетенций содержится в разделе 3 Рабочей программы дисциплины «Компетенции обучающегося, формируемые в результате освоения дисциплины»:

ПК-1 – способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;		
Знать	Уметь	Владеть
- основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - методы концептуального проектирования технологий обеспечения информационной безопасности; - основные угрозы безопасности информации и модели нарушителя в компьютерных системах; принципы формирования политики информационной безопасности в компьютерных системах; - методы аттестации уровня защищенности компьютерных систем; - основные методы управления информационной безопасностью	- осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; - организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности;- разрабатывать модели угроз и нарушителей информационной безопасности компьютерных систем; - разрабатывать частные политики информационной безопасности компьютерных х систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности компьютерных систем; - оценивать информационные риски в компьютерных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем	- методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных компьютерных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной безопасностью компьютерных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками организации и обеспечения режима секретности; - навыками управления информационной безопасностью простых объектов

ПК-2 – способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;		
Знать	Уметь	Владеть
- основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - методы концептуального проектирования технологий обеспечения информационной безопасности; - основные угрозы безопасности информации и модели нарушителя в компьютерных системах; принципы формирования политики информационной безопасности в компьютерных системах; - методы аттестации уровня защищенности компьютерных систем; -	- осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; - организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности;- разрабатывать модели угроз и нарушителей информационной безопасности компьютерных систем; - разрабатывать частные политики информационной безопасности компьютерных х систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности компьютерных систем; - оценивать информационные риски в компьютерных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем; - составлять аналитические обзоры по вопросам обеспечения	- методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных компьютерных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной безопасностью компьютерных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью

основные методы управления информационной безопасностью	информационной безопасности компьютерных систем	служб защиты информации на предприятии; - навыками организации и обеспечения режима секретности; - навыками управления информационной безопасностью простых объектов

ПК-3 – способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.		
Знать	Уметь	Владеть
- основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - методы концептуального проектирования технологий обеспечения информационной безопасности; - основные угрозы безопасности информации и модели нарушителя в компьютерных системах; принципы формирования политики информационной безопасности в компьютерных системах; - методы аттестации уровня защищенности компьютерных систем; - основные методы управления информационной безопасностью	- осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; - организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности;- разрабатывать модели угроз и нарушителей информационной безопасности компьютерных систем; - разрабатывать частные политики информационной безопасности компьютерных х систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности компьютерных систем; - оценивать информационные риски в компьютерных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем	- методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных компьютерных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной безопасностью компьютерных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками организации и обеспечения режима секретности; - навыками управления информационной безопасностью простых объектов

Оценка по дисциплине выставляется с учетом среднего балла освоения компетенций, формируемых дисциплиной, при условии сформированности каждой компетенции не ниже порогового уровня.

3. Показатели, критерии и шкала оценивания компетенций текущего контроля знаний по учебной дисциплине «Технологии обеспечения информационной безопасности»

Текущий контроль знаний, согласно «Положению о рейтинговой системе комплексной оценки знаний студентов в ВлГУ» (далее Положение) в рамках изучения дисциплины «Технологии обеспечения информационной безопасности» предполагает письменный рейтинг-контроль, выполнение и защиту лабораторных, а также выполнение самостоятельных работ. В случае использования при изучении дисциплины дистанционных образовательных технологий проводится компьютерное тестирование.

Регламент проведения письменного рейтинг-контроля

№	Вид работы	Продолжительность
1	Предел длительности рейтинг-контроля	35-40 мин.
2	Внесение исправлений	до 5 мин.

	Итого	до 45 мин.

Критерии оценки письменного рейтинг-контроля

Результаты каждого письменного рейтинга оцениваются в баллах. Максимальная сумма, набираемая студентом на каждом письменном рейтинге, составляет 10 баллов.

Критерии оценки для письменного рейтинга:

- 9-10 баллов выставляется обучающемуся, если соблюдаются критерии: полное раскрытие темы, вопроса, указание точных названий и определений, правильная формулировка понятий и категорий, приведение формул и (в необходимых случаях) их вывода, приведение статистики, самостоятельность ответа, использование дополнительной литературы;

- 7-8 баллов выставляется обучающемуся, если соблюдаются критерии: недостаточно полное раскрытие темы, несущественные ошибки в определении понятий и категорий, формулах, выводе формул, статистических данных, кардинально не меняющих суть изложения, наличие грамматических и стилистических ошибок, использование устаревшей учебной литературы;

- 5-6 баллов выставляется обучающемуся, если соблюдаются критерии: отражение лишь общего направления изложения лекционного материала и материала современных учебников, наличие достаточно количества несущественных или одной-двух существенных ошибок в определении понятий и категорий, формулах, их выводе, статистических данных, наличие грамматических и стилистических ошибок, использование устаревшей учебной литературы, неспособность осветить проблематику дисциплины;

- 1-4 балла выставляется обучающемуся, если соблюдаются критерии: нераскрытые темы; большое количество существенных ошибок, наличие грамматических и стилистических ошибок, отсутствие необходимых умений и навыков.

Оценочные средства для текущего контроля знаний по учебной дисциплине «Технологии обеспечения информационной безопасности» (письменный рейтинг-контроль)

1 семестр:

Перечень вопросов для текущего контроля (письменный рейтинг №1):

1. Основные технические сервисы защиты информации в компьютерных системах.
2. Принципы построения программных продуктов в защищенном исполнении.
3. Идентификация, аутентификация и контроль доступа.
4. Защита распределенных информационных систем и обеспечение безопасности взаимодействия компонентов этих систем.
5. "Слабые" протоколы аутентификации.
6. Парольная аутентификация.
7. Проблема хранения и передачи паролей.
8. Хеширование паролей.
9. Использование имитовставки для повышения стойкости к подбору паролей.
10. Парольная политика.

Перечень вопросов для текущего контроля (письменный рейтинг №2):

1. Двухфакторная аутентификация.
2. PIN-коды и одноразовые пароли.
3. Вычисляемые ключи.
4. Схема Лэмпорта.
5. Атаки подбора паролей напрямую.

6. Атаки подбора паролей по словарю.
7. Гибридная атака, атака повтора пароля, pass the hash.
8. "Сильные" протоколы аутентификации.
9. Протоколы типа "запрос-ответ".
10. Аутентификация на основе симметричного шифрования

Перечень вопросов для текущего контроля (письменный рейтинг №3):

1. Аутентификация на основе асимметричного шифрования.
2. Протоколы ISO 9798
3. Схема Нидхэма-Шрёдера.
4. Применение "сильных" схем аутентификации в аппаратных ключах.
5. Протоколы аутентификации с нулевым разглашением.
6. Протокол Фиата-Шамира.
7. Протокол Фейге-Фиата-Шамира.
8. Схема GQ
9. Протокол аутентификации Шнорра.
10. Атаки на протоколы аутентификации.

2 семестр:

Перечень вопросов для текущего контроля (письменный рейтинг №1):

1. Атака имперсонации
2. Атака повторной отправки
3. Атаки перемежения.
4. Атаки отражения
5. Атака вынужденной задержки
6. Модели контроля доступа в компьютерных системах
7. Задача контроля доступа.
8. Классификация моделей управления доступом.
9. Автоматная модель доступов в информационной системе.
10. Понятия субъекта и объекта доступа.

Перечень вопросов для текущего контроля (письменный рейтинг №2):

1. Канал утечки по памяти
2. Канал утечки по времени
3. Дискреционное управление доступом.
4. Матрица доступа.
5. Модель Харрисона-Руззо-Ульмана.
6. Понятие утечки права.
7. Модель типизированной матрицы доступов.
8. Понятие передачи прав.
9. Базовая и расширенная модель take-grant.
10. Мандатное управление доступом.

Перечень вопросов для текущего контроля (письменный рейтинг №3):

1. Понятие решетки уровней конфиденциальности.
2. Модель Белла-Лападула.
3. Политика high-watermark и low-watermark.
4. Модель контроля целостности Биба.
5. Вопросы вычислительной сложности верификации исходных условий в мандатном управлении доступом.
6. Ролевое разграничение доступа.
7. Модель администрирования РРД,
8. Дискреционная модель ролевого разграничения доступа.
9. Мандатная модель ролевого разграничения доступа
10. Контроль доступа в современных информационных системах.

Регламент проведения лабораторных работ

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Технологии обеспечения информационной безопасности» предполагается выполнение лабораторных работ, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

Критерии оценки выполнения лабораторных работ (1 семестр)

Результаты выполнения каждой лабораторной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение каждой лабораторной работы, составляет 6 баллов.

Критерии оценки для выполнения лабораторной работы:

- 4-6 баллов выставляется обучающемуся, если соблюдаются критерии: представлен полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения и надлежащим образом оформленный (в печатном или электронном виде - в соответствие с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся верно и полно ответил на все контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно и в определенный преподавателем срок;

- 3-3,9 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствие с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся преимущественно верно и полно ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно, возможно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки;

- 2-2,9 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание не всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствие с требованием преподавателя), в основном выполнено задание на лабораторную работу, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с отражением лишь общего направления изложения материала, с наличием достаточно количества несущественных или одной-двух существенных ошибок, лабораторная работа выполнена самостоятельно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература;

- 0,9-1,9 балла выставляется обучающемуся, если соблюдаются критерии: письменный отчет по лабораторной работе (в печатном или электронном виде - в соответствие с требованием преподавателя) не представлен или представлен неполный, отчет содержит описание не всех этапов выполнения работы, имеет погрешности в оформлении, задание на лабораторную работу выполнено не полностью, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с большим количеством существенных ошибок, продемонстрировал неспособность осветить

проблематику лабораторной работы, лабораторная работа выполнена несамостоятельно, с существенным нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература, обучающийся при выполнении работы продемонстрировал отсутствие необходимых умений и практических навыков.

При оценке за лабораторную работу менее 0,9 балла, данная работа считается невыполненной и не зачитывается. При невыполнении лабораторной работы хотя бы по одной из изучаемых тем, обучающийся не получает положительную оценку при промежуточном контроле по дисциплине (зачет).

Критерии оценки выполнения лабораторных работ (2 семестр)

Результаты выполнения каждой лабораторной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение каждой лабораторной работы, составляет 2 балла.

Критерии оценки для выполнения лабораторной работы:

- 1,5-2 балла выставляется обучающемуся, если соблюдаются критерии: представлен полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения и надлежащим образом оформленный (в печатном или электронном виде - в соответствие с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся верно и полно ответил на все контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно и в определенный преподавателем срок;

- 0,9-1,4 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствие с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся преимущественно верно и полно ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно, возможно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки;

- 0,5-0,8 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание не всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствие с требованием преподавателя), в основном выполнено задание на лабораторную работу, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с отражением лишь общего направления изложения материала, с наличием достаточно количества несущественных или одной-двух существенных ошибок, лабораторная работа выполнена самостоятельно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература;

- 0,1-0,4 балла выставляется обучающемуся, если соблюдаются критерии: письменный отчет по лабораторной работе (в печатном или электронном виде - в соответствие с требованием преподавателя) не представлен или представлен неполный, отчет содержит

описание не всех этапов выполнения работы, имеет погрешности в оформлении, задание на лабораторную работу выполнено не полностью, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с большим количеством существенных ошибок, продемонстрировал неспособность осветить проблематику лабораторной работы, лабораторная работа выполнена несамостоятельно, с существенным нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература, обучающийся при выполнении работы продемонстрировал отсутствие необходимых умений и практических навыков.

При оценке за лабораторную работу менее 0,1 балла, данная работа считается невыполненной и не зачитывается. При невыполнении лабораторной работы хотя бы по одной из изучаемых тем, обучающийся не получает положительную оценку при промежуточном контроле по дисциплине (экзамене).

Оценочные средства для текущего контроля знаний по учебной дисциплине «Технологии обеспечения информационной безопасности» (лабораторные работы)

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ (1 семестр):

Лабораторная работа №1. Создание программного модуля парольной аутентификации. Пароль передается и хранится в виде значения односторонней функции от строки, введенной пользователем. Хранение пароля следует осуществлять в зашифрованном key-value хранилище.

Лабораторная работа №2. Создание программного модуля двухфакторной аутентификации по схеме Лэмпорта с генерацией одноразовых паролей. Пароль передается и хранится в виде значения односторонней функции от строки, введенной пользователем. Хранение пароля следует осуществлять в зашифрованном key-value хранилище.

Лабораторная работа №3. Создание программного модуля генерации пары ключей для асимметричных криптосистем. Пара ключей должна быть снабжена сертификатом формата X.509. Размер ключа принять равным или более 128 бит.

Лабораторная работа №4. Создание программного модуля, поддерживающего протоколы аутентификации стандарта 9798-2 и 9798-3. Транзакции следует осуществлять поверх протокола безопасности транспортного уровня TLS. Для реализации криптографических примитивов рекомендуется воспользоваться библиотекой OpenSSL.

Лабораторная работа №5. Создание программного модуля, поддерживающего один из протоколов аутентификации с нулевым разглашением (на выбор). Протестировать его в отношении технологической устойчивости к основным атакам на схемы аутентификации

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ (2 семестр):

Лабораторная работа №1. Построение проекта архитектуры сервиса хранения файлов в защищенном исполнении. Сервис должен поддерживать шифрование файлов, аутентификацию с нулевым разглашением и мандатную модель контроля доступа.

Лабораторная работа №2. Разработка технического задания на сервис хранения файлов в защищенном исполнении. Сервис должен иметь возможность параллельной работы более 10 клиентов и предусматривать возможность передачи файлов между пользователями.

Лабораторная работа №3. Реализация каркаса приложений клиента и сервера для хранения файлов. Проектирование пользовательского интерфейса для клиента и сервера.

Лабораторная работа №4. Разработка протокола обмена сообщениями между клиентом и сервером. Разработка и реализация структуры базы данных для хранения файлов и пользовательских данных.

Лабораторная работа №5. Реализация модуля шифрования содержимого базы данных. Оценка утечки данных в случае компрометации клиента, сервера, пользовательских аутентификаторов, канала связи.

Лабораторная работа №6. Реализация модели контроля доступа. Написание методов для основных процедур передачи прав, назначения мандатов субъектов и объектов, сброса мандатов в соответствии с политикой low-watermark

Лабораторная работа №7. Реализация модуля аутентификации. Написание процедур, осуществляющих создание и хранение аутентификаторов пользователей. Реализация защищенного обмена аутентификаторами.

Лабораторная работа №8. Реализация административных процедур для сервиса хранения файлов в защищенном исполнении - создания, удаления пользователей, выделения им дисковой квоты и т. д.

Лабораторная работа №9. Тестирование сервиса хранения файлов в защищенном исполнении, в том числе и в отношении технологической устойчивости к основным атакам на схемы аутентификации.

Регламент проведения самостоятельной работы

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Технологии обеспечения информационной безопасности» предполагается выполнение заданий СРС, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

Критерии оценки выполнения самостоятельной работы (1 семестр)

Результаты выполнения самостоятельной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение работы по каждой теме, составляет 3 балла.

Критерии оценки для выполнения работы:

- 2,4-3 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся верно и полно ответил на все контрольные вопросы преподавателя по теме; полностью, самостоятельно и в определенный преподавателем срок выполнено задание;

- 1,4-2,3 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся преимущественно верно и полно ответил на контрольные вопросы преподавателя по теме; задание выполнено самостоятельно, возможно, с нарушением определенного преподавателем срока;

- 0,7-1,3 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся ответил на контрольные вопросы преподавателя по теме с отражением лишь общего направления изложения материала; задание выполнено самостоятельно, возможно, с нарушением определенного преподавателем срока, содержит незначительные ошибки;

- 0,2-0,6 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся ответил на контрольные вопросы преподавателя по теме с большим количеством существенных ошибок, продемонстрировал неспособность осветить проблематику темы; задание выполнено не полностью, не самостоятельно, с существенным нарушением определенного преподавателем срока, при выполнении задания продемонстрировал отсутствие необходимых умений и практических навыков.

Оценочные средства для текущего контроля знаний по учебной дисциплине «Технологии обеспечения информационной безопасности» (самостоятельная работа)

1 семестр:

№ пп	Раздел (тема) дисциплины	Виды СРС	Формы контроля СРС	Баллы по СРС
1	Введение. Основные технические сервисы защиты информации в компьютерных системах.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
2	"Слабые" протоколы аутентификации Парольная аутентификация	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
3	Двухфакторная аутентификация PIN-коды и одноразовые пароли.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
4	"Сильные" протоколы аутентификации Протоколы типа "запрос-ответ".	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
5	Протоколы аутентификации с нулевым разглашением.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
6	Модели контроля доступа в компьютерных системах. Общие сведения о задаче КД.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
7	Дискреционное управление доступом.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
8	Мандатное управление доступом.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
9	Ролевое разграничение доступа. Модель администрирования РРД, дискреционная и мандатная модели	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
			Итого за семестр:	27

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении СРС (1 семестр):

- Принципы и технологии построения DLP-систем.
- Аппаратные и программные межсетевые экраны
- Системы протоколирования событий в информационных системых
- Ролевое разграничение доступа в СУБД Oracle
- Ролевое разграничение доступа в СУБД MS SQL Server
- Экранирование и фильтрация запросов на уровне приложений
- Алгоритм шифрования AES
- Протоколы безопасности транспортного уровня
- Протокол аутентификации LDAP
- Протокол аутентификации Kerberos
- Система аутентификации Radius
- Single Sign-on в Windows-сетях
- Способы организации сессий в Web-сервисах
- Аутентификация в Web-сервисах
- Протокол Oauth2
- Способы хранения аутентификаторов в Windows
- Способы хранения аутентификаторов в GNU/Linux
- Контексты безопасности SELinux
- Модель изолированной программной среды

- Модель системы военных сообщений
- Модель Кларка-Уилсона
- Атаки типа "человек посередине"
- Аппаратные ключи eToken
- Виды программных закладок и бэкдоров.
- Протокол Диффи-Хеллмана
- Схема Нидхэма-Шредера
- Аутентификация в аппаратных токенах
- Особенности доверенной третьей стороны в протоколах аутентификации
- Принципы протоколов с нулевым разглашением
- Протокол Фиата-Шамира
- Протокол Фейге-Фиата-Шамира
- Протокол GQ
- Протокол Шнорра
- Атаки на протоколы аутентификации
- Задача контроля доступа
- Основные принципы управления доступом в компьютерных системах
- Понятие субъекта и объекта доступа
- аналы утечки по памяти и по времени
- Классификация моделей управления доступом
- Матрица доступа
- Модель Харрисона-Руззо-Ульмана
- Утечка права
- Вычислительная сложность верификации по дискреционным моделям
- Модель типизированной матрицы доступов
- Модель take-grant
- Решетка уровней конфиденциальности
- Модель Белла-Лападула
- Модель целостности Биба
- Политика high-watermark и low-watermark
- Дискреционное ролевое разграничение доступа
- Мандатное ролевое разграничение доступа
- Управление доступом в современных информационных системах

Регламент проведения курсового проекта (2 семестр)

Курсовая работа заключается в создании программного комплекса, реализующего защищенное хранение файлов. Программный комплекс должен быть реализован с использованием архитектуры "клиент-сервер" и содержать механизмы аутентификации, шифрования и управления доступом.

Протокол аутентификации с нулевым разглашением, используемая криптосистема и модель контроля доступа выбирается по желанию студента из рассмотренных в курсе лекций.

Работу можно разбить на ряд этапов:

- построение проекта архитектуры сервиса хранения файлов;
- разработку технического задания на сервис хранения файлов;
- реализацию каркаса приложений клиента и сервера для хранения файлов;
- проектирование пользовательского интерфейса для клиента и сервера;
- реализацию модуля шифрования содержимого базы данных;
- написание методов для основных процедур передачи прав, назначения мандатов субъектов и объектов, сброса мандатов в соответствии с политикой low-watermark;
- реализацию модуля аутентификации;

- реализацию административных процедур для сервиса;
- тестирование и отладку.

Критерии оценки выполнения курсового проекта

№п/п	Расшифровка критериев	Количество баллов
1	Представление результатов курсовой работы (доклад, ответы на вопросы)	20
2	Качество оформления пояснительной записки и графического материала (в т.ч. презентации). Нормоконтроль в соответствии с требованиями ГОСТ.	30
3	Промежуточная аттестация (оцениваются результаты работы: степень выполнения, соответствие поставленной задаче, график работ, устранение замечаний и т.п.)	25
4	Финальная аттестация (оцениваются результаты работы: степень выполнения, соответствие поставленной задаче, разработанное ПО и т.п.)	25
	Общее количество баллов	100

Баллы округляются в большую строну. Результаты курсового проекта определяются следующими оценками: «зачтено» и «незачтено» по следующей шкале:

«Зачтено» - от 61 балла.

«Незачтено» - 60 и менее баллов.

При неудовлетворительной оценке за курсовой проект обучающийся не получает положительную оценку при промежуточном контроле по дисциплине (экзамене).

Общее распределение баллов текущего контроля по видам учебных работ для студентов (в соответствие с Положением)

1 семестр

№	Пункт	Максимальное число баллов
1	Письменный рейтинг-контроль 1	10
2	Письменный рейтинг-контроль 2	10
3	Письменный рейтинг-контроль 3	10
4	Посещение занятий студентом	8
5	Дополнительные баллы (бонусы)	5
6	Лабораторные работы	30
7	Выполнение семестрового плана самостоятельной работы	27
	Всего	100

2 семестр

№	Пункт	Максимальное число баллов
1	Письменный рейтинг-контроль 1	10
2	Письменный рейтинг-контроль 2	10
3	Письменный рейтинг-контроль 3	10
4	Посещение занятий студентом	6

5	Дополнительные баллы (бонусы)	6
6	Лабораторные работы	18
7	Экзамен	40
	Всего	100

4. Показатели, критерии и шкала оценивания компетенций промежуточной аттестации знаний по учебной дисциплине «Технологии обеспечения информационной безопасности»

Регламент проведения промежуточного контроля (зачета)

Промежуточная аттестация по итогам освоения дисциплины (зачет) проводится перед экзаменационной сессией. Зачет проставляется студенту после выполнения студентом семестрового плана самостоятельной работы.

Критерии оценивания при проставлении зачета (1 семестр)

Критерии оценки для промежуточного контроля (зачета):

- оценка «отлично» (соответствует 91-100 баллов по шкале рейтинга) выставляется обучающемуся, если соблюдаются критерии: теоретическое содержание оцениваемой части дисциплины освоено полностью, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены в установленные сроки, качество их выполнения оценено числом баллов, близким к максимальному;

- оценка «хорошо» (соответствует 74-90 баллов по шкале рейтинга) выставляется обучающемуся, если соблюдаются критерии: теоретическое содержание курса освоено полностью, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками или с нарушением установленных сроков;

- оценка «удовлетворительно» (соответствует 61-73 баллов по шкале рейтинга) выставляется обучающемуся, если соблюдаются критерии: теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки;

- оценка «неудовлетворительно» (соответствует менее 60 баллов по шкале рейтинга) выставляется обучающемуся, если соблюдаются критерии: теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки.

Оценочные средства для промежуточной аттестации по учебной дисциплине «Технологии обеспечения информационной безопасности» (зачёт)

Перечень вопросов для промежуточного контроля (зачета)

1. Основные технические сервисы защиты информации в компьютерных системах.
2. Принципы построения программных продуктов в защищенном исполнении.
3. Идентификация, аутентификация и контроль доступа.
4. Защита распределенных информационных систем и обеспечение безопасности взаимодействия компонентов этих систем.

5. "Слабые" протоколы аутентификации.
6. Парольная аутентификация.
7. Проблема хранения и передачи паролей.
8. Хеширование паролей.
9. Использование имитовставки для повышения стойкости к подбору паролей.
10. Парольная политика.
11. Двухфакторная аутентификация.
12. PIN-коды и одноразовые пароли.
13. Вычисляемые ключи.
14. Схема Лэмпорта.
15. Атаки подбора паролей напрямую.
16. Атаки подбора паролей по словарю.
17. Гибридная атака, атака повтора пароля, pass the hash.
18. "Сильные" протоколы аутентификации.
19. Протоколы типа "запрос-ответ".
20. Аутентификация на основе симметричного шифрования
21. Аутентификация на основе асимметричного шифрования.
22. Протоколы ISO 9798
23. Схема Нидхэма-Шрёдера.
24. Применение "сильных" схем аутентификации в аппаратных ключах.
25. Протоколы аутентификации с нулевым разглашением.
26. Протокол Фиата-Шамира.
27. Протокол Фейге-Фиата-Шамира.
28. Схема GQ
29. Протокол аутентификации Шнорра.
30. Атаки на протоколы аутентификации.

Регламент проведения промежуточного контроля (экзамена)

Промежуточная аттестация по итогам освоения дисциплины (экзамен) проводится в экзаменационную сессию. Экзамен проводится по билетам, содержащим три вопроса. Студент пишет ответы на вопросы экзаменационного билета на листах белой бумаги формата А4, на каждом из которых должны быть указаны: фамилия, имя отчество студента; шифр студенческой группы; дата проведения экзамена; номер экзаменационного билета. Листы должны быть подписаны и студентом и экзаменатором после получения студентом экзаменационного билета. Экзаменационные билеты должны быть оформлены в соответствие с утвержденным регламентом.

После подготовки студент устно отвечает на вопросы билета и уточняющие вопросы экзаменатора. Экзаменатор вправе задать студенту дополнительные вопросы и задания по материалам дисциплины для выявления степени усвоения студентом компетенций.

Максимальное количество баллов, которое студент может получить на экзамене, в соответствие с Положением составляет 40 баллов.

Критерии оценивания компетенций на экзамене (2 семестр)

Оценка в баллах	Оценка за ответ на экзамене	Критерии оценивания компетенций
30 - 40	«Отлично»	Студент глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при

		видоизменении заданий, использует при ответе материалы из основной и дополнительной литературы по дисциплине, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач, подтверждает полное освоение компетенций, предусмотренных рабочей программой дисциплины.
20 - 29	«Хорошо»	Студент показывает твердое знание материала, грамотно и по существу излагает его, не допускает существенных неточностей при ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, допуская некоторые неточности; демонстрирует хороший уровень освоения материала, информационной и коммуникативной культуры и в целом подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины.
10 - 19	«Удовлетворительно»	Студент показывает знания только основного материала, но не усвоил его деталей; допускает неточности, недостаточно правильные формулировки, которые в целом не препятствуют усвоению последующего программного материала; допускает нарушения логической последовательности в изложении программного материала; испытывает затруднения при выполнении практических работ; подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины, на минимально допустимом уровне.
0 - 10	«Неудовлетворительно»	Студент не знает значительной части программного материала, имеет менее 50% правильно выполненных заданий от общего объема работы, допускает существенные ошибки при изложении материала, неуверенно, с большими затруднениями выполняет практические работы, не подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины.

Оценочные средства для промежуточной аттестации по учебной дисциплине «Технологии обеспечения информационной безопасности» (экзамен)

Перечень вопросов для промежуточного контроля (экзамена)

1. Идентификация, аутентификация и контроль доступа.
2. Модель нарушителя в компьютерных системах.
3. Основные сценарии атак в компьютерных системах.
4. Хэширование паролей
5. Хранение паролей.
6. Сложность подбора пароля.
7. Двухфакторная аутентификация.
8. Схема Лэмпорта
9. Одноразовые пароли с доставкой по выделенному каналу связи
10. Парольная политика.
11. Использование "соли" для предотвращения атаки подбора пароля
12. Атаки повтора пароля и pass the hash
13. Схемы аутентификации ISO 9798
14. Основные принципы "сильной" аутентификации
15. Протокол Диффи-Хеллмана
16. Схема Нидхэма-Шредера

17. Аутентификация в аппаратных токенах
18. Особенности доверенной третьей стороны в протоколах аутентификации
19. Принципы протоколов с нулевым разглашением
20. Протокол Фиата-Шамира
21. Протокол Фейге-Фиата-Шамира
22. Протокол GQ
23. Протокол Шнорра
24. Атаки на протоколы аутентификации
25. Задача контроля доступа
26. Основные принципы управления доступом в компьютерных системах
27. Понятие субъекта и объекта доступа
28. Каналы утечки по памяти и по времени
29. Классификация моделей управления доступом
30. Матрица доступа
31. Модель Харрисона-Руззо-Ульмана
32. Утечка права
33. Вычислительная сложность верификации по дискреционным моделям
34. Модель типизированной матрицы доступов
35. Модель take-grant
36. Решетка уровней конфиденциальности
37. Модель Белла-Лападула
38. Модель целостности Биба
39. Политика high-watermark и low-watermark
40. Дискреционное ролевое разграничение доступа
41. Мандатное ролевое разграничение доступа
42. Управление доступом в современных информационных системах