МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА»

Кафедра «Информационные системы в экономике»

УТВЕРЖДЕН

на заседании кафедры
«02» 09 2023 г., протокол № 1

Заведующий кафедрой
_____ Л.Р. Магомаева
(подпись)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Информационная безопасность в цифровой экономике»

Направление подготовки
38.03.05. - «Бизнес-информатика»

Направленность (профиль)
«Управление ИТ-проектами»

Квалификация
бакалавр

Год начала подготовки: 2023

Составитель _____ М.К. Абдулаев
(подпись)

Грозный – 2023

Паспорт фонда оценочных средств по дисциплине

«Информационная безопасность»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Введение в информационную безопасность	ОПК-4, ПК-3	Тестирование
2	Задачи и методы информационной безопасности	ОПК-4, ПК-3	Тестирование
3	Угрозы информационной безопасности	ОПК-4, ПК-3	Опрос Проверка выполнения лабораторной работы
4	Потенциальные противники и атаки	ОПК-4, ПК-3	Тестирование
5	Стандарты обеспечения ИБ	ОПК-4, ПК-3	Тестирование
6	Организационно-правовые методы информационной безопасности	ОПК-4, ПК-10	Опрос
7	Законодательный уровень информационной безопасности	ОПК-4, ПК-3	Проверка выполнения лабораторной работы
8	Административный уровень информационной безопасности	ОПК-4, ПК-3	Опрос
9	Основные положения теории информационной безопасности информационных систем	ОПК-4, ПК-3	Проверка выполнения лабораторной работы
10	Основные технологии построения защищенных экономических информационных систем.	ОПК-4, ПК-3	Опрос
11	Управление рисками	ОПК-4, ПК-3	Проверка выполнения лабораторной работы
12	Процедурный уровень информационной безопасности	ОПК-4, ПК-3	Опрос
13	Программно-технические методы защиты	ОПК-4, ПК-3	Проверка выполнения лабораторной работы
14	Идентификация и аутентификация	ОПК-4, ПК-3	Опрос
15	Сервисы управления доступом	ОПК-4, ПК-3	Проверка выполнения лабораторной работы
16	Протоколирование и аудит	ОПК-4, ПК-3	Опрос

17	Экранирование и анализ защищенности	ОПК-4, ПК-3	Проверка выполнения лабораторной работы
18	Тунелирование и управление	ОПК-4, ПК-3	Опрос
19	Обеспечение высокой доступности	ОПК-4, ПК-3	Проверка выполнения лабораторной работы
20	Криптографические методы защиты	ОПК-4, ПК-3	Опрос

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	*Лекция*	Устное систематическое и последовательное изложение материала по какой-либо проблеме, методу, теме вопроса и т. д.	Устное изложение, публичное чтение /по разделам
2	*Лабораторная работа*	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом	Комплект заданий для выполнения лабораторных работ
3	*Рубежный контроль*	Форма проверки знаний по дисциплине в виде первой и второй рубежных аттестаций	Вопросы к аттестациям
4	*Зачет/Экзамен*	Итоговая форма оценки знаний	Вопросы к зачету/экзамену

Оценки за устный опрос и защиту лабораторных работ выставляются преподавателем в соответствии со шкалой баллов БРС данной дисциплины! Баллы за устный опрос и защиту лабораторных работ выставляются в графу текущей аттестации (от 0 – 15 баллов за семестр).

ЗАДАНИЯ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

7 семестр

Лабораторная работа №1. Установка и удаление сертификатов. (ОПК-4)

Лабораторная работа №2. Настройка уровня безопасности, конфиденциальности и эффективности работы программы INTERNET EXPLORER. (ПК-3)

Лабораторная работа №3. Анализ угроз и защищенности объекта (ПК-3)

8 семестр

Лабораторная работа №4. Создание самоподписанных сертификатов. (ПК-3)

Лабораторная работа №5. Использование электронных идентификаторов Рутокен и JaCarta. (ПК-3)

Лабораторная работа №6.
Шифрование данных. Использование ПО КриптоАРМ. (ПК-3)

Критерии оценки

Регламентом БРС предусмотрено всего 15 баллов за текущую работу студента. Критерии оценки разработаны, исходя из возможности ответа студентом до 5 лекций с использованием дополнительного материала по ним. (по 3 баллов).

✓ ***0 баллов выставляется студенту, если*** *подготовлен некачественный ответ: тема не раскрыта*, в изложении темы отсутствует четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений.

✓ ***1- балл выставляется студенту, если*** *подготовлен некачественный ответ по теме: тема раскрыта, однако в изложении материала отсутствует четкая структура* отражающая сущность раскрываемых понятий, теорий, явлений.

✓ ***2 балла выставляется студенту, если*** *подготовлен качественный ответ:* тема хорошо раскрыта, в изложении материала прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Студент хорошо апеллирует терминами дисциплины. Однако затрудняется ответить на дополнительные вопросы по теме (1-2 вопроса).*

✓ ***3 балла выставляется студенту, если*** *подготовлен качественный ответ:* тема хорошо раскрыта, в изложении материала прослеживается четкая структура логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Студент свободно апеллирует терминами дисциплины, демонстрирует авторскую позицию. Способен ответить на дополнительные вопросы по теме (1-2 вопроса).*

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт цифровых технологий и технологического предпринимательства

Кафедра информационные системы в экономике

ЗАЧЕТНО-ЭКЗАМЕНАЦИОННЫЕ МАТЕРИАЛЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Информационная безопасность»

Вопросы к первой рубежной аттестации 7 семестр

1. Введение в информационную безопасность (ОПК-4)
2. Задачи и методы информационной безопасности (ПК-3)
3. Угрозы информационной безопасности (ПК-3)
4. Потенциальные противники и атаки
5. Стандарты обеспечения ИБ
6. Организационно-правовые методы информационной безопасности

Вопросы ко второй рубежной аттестации 7 семестр

1. Законодательный уровень информационной безопасности (ОПК-4)
2. Административный уровень информационной безопасности
3. Основные положения теории информационной безопасности информационных систем
4. Основные технологии построения защищенных экономических информационных систем. ПК-3
5. Модель угроз информации на территории РФ
6. Способы защиты операционных систем (ОПК-4)
7. Анализ мирового рынка антивирусного программного обеспечения
8. Компьютерная преступность в России (ОПК-4)

Вопросы к первой рубежной аттестации 8 семестр

1. Управление рисками (ПК-3)
2. Процедурный уровень информационной безопасности
3. Программно-технические методы защиты

4. Идентификация и аутентификация (ПК-3)
5. Сервисы управления доступом

Вопросы ко второй рубежной аттестации 8 семестр

1. Протоколирование и аудит (ПК-3)
2. Экранирование и анализ защищенности
3. Тунелирование и управление (ОПК-4)
4. Обеспечение высокой доступности
5. Криптографические методы защиты (ПК-3)

Вопросы к зачету (7семестр)

1. Введение в информационную безопасность (ОПК-4)
2. Задачи и методы информационной безопасности (ПК-3)
3. Угрозы информационной безопасности (ПК-3)
4. Потенциальные противники и атаки
5. Стандарты обеспечения ИБ
9. Законодательный уровень информационной безопасности (ОПК-4)
10. Административный уровень информационной безопасности
11. Основные положения теории информационной безопасности информационных систем
12. Основные технологии построения защищенных экономических информационных систем.
13. Модель угроз информации на территории РФ
14. Способы защиты операционных систем
15. Анализ мирового рынка антивирусного программного обеспечения
16. Компьютерная преступность в России (ОПК-4)

Вопросы к экзамену

1. Управление рисками ПК-3
2. Процедурный уровень информационной безопасности
3. Программно-технические методы защиты
4. Идентификация и аутентификация (ПК-3)

5. Сервисы управления доступом
6. Протоколирование и аудит (ПК-3)
7. Экранирование и анализ защищенности
8. Тунелирование и управление (ОПК-4)
9. Обеспечение высокой доступности
10. Криптографические методы защиты (ПК-3)
11. Протоколирование и аудит
12. Экранирование и анализ защищенности

Критерии оценки знаний студента на зачете

Оценка «зачтено» - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «не зачтено» - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

Критерии оценки знаний студента на экзамене

Оценка «отлично» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка «хорошо» - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка «удовлетворительно» - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых

понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «неудовлетворительно» - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

ТЕМЫ ДОКЛАДОВ (РЕФЕРАТОВ) ПО ДИСЦИПЛИНЕ

«Информационная безопасность»

Вопросы для рефератов

Этапы работы над рефератом

1. Сформулируйте тему. Тема должна быть не только актуальной по своему значению, но оригинальной, интересной по содержанию.

2. Подберите и изучите основные источники по теме (как правило, не менее 8-10).

3. Составьте библиографию.

4.Обработайте и систематизируйте информацию.

5.Разработайте план реферата.

6. Напишите реферат.

7.Выступите с результатами исследования в аудитории на семинарском занятии, заседании предметного кружка, студенческой научно-практической конференции.

Содержание работы должно отражать:

- ✓ знание современного состояния проблемы;
- ✓ обоснование выбранной темы;
- ✓ использование известных результатов и фактов;
- ✓ полноту цитируемой литературы, ссылки на работы ученых, занимающихся данной проблемой;
- ✓ актуальность поставленной проблемы;
- ✓ материал, подтверждающий научное, либо практическое значение в настоящее время.

Требования к оформлению и защите реферативных работ

1. Общие положения:

1.1.Защита реферата предполагает предварительный выбор студентом интересующей его темы работы с учетом рекомендаций преподавателя, последующее глубокое изучение избранной для реферата проблемы, изложение выводов по теме реферата. Выбор предмета и темы реферата осуществляется студентом в начале изучения дисциплины. Не позднее, чем за 2 дня до защиты или выступления реферат

представляется на рецензию преподавателю. Оценка выставляется при наличии рецензии и после защиты реферата. Работа представляется в отдельной папке.

1.2. Объем реферата – 15-20 страниц текста, оформленного в соответствии с требованиями.

1.3. В состав работы входят:

- ✓ реферат;
- ✓ рецензия преподавателя на реферат (представляет отдельный документ).

2. Требования к тексту.

2.1. Реферат выполняется на стандартных страницах белой бумаги формата А-4 (верхнее, нижнее поля – 2см, правое поле – 1,5 см; левое – 3 см).

2.2.Текст печатается обычным шрифтом Times New Roman (размер шрифта – 14 кегль). Заголовки – полужирным шрифтом Times New Roman (размер шрифта – 14 кегль).

2.3.Интервал между строками – полуторный.

2.4.Текст оформляется на одной стороне листа.

2.5.Формулы, схемы, графики вписываются черной пастой (тушью), либо выполняются на компьютере.

Критерии оценки учебного реферата.

- ✓ соответствие темы реферата содержанию;
- ✓ достаточность и современность привлеченных к рассмотрению источников;
- ✓ аналитичность работы;
- ✓ методологическая корректность;
- ✓ нетривиальность суждений;
- ✓ новизна взгляда;
- ✓ обоснованность выводов;
- ✓ логичность построения, проблемно-поисковый характер изложения материала;
- ✓ использование понятийного аппарата;
- ✓ соответствие стандарту стиля работы и оформления реферата.

Темы для рефератов 7,8 семестр

№ п/п	Темы для самостоятельного изучения
1.	Обеспечение информационной безопасности в банковских и финансовых структурах
2.	Анализ мирового рынка биометрических систем, используемых в системах обеспечения информационной безопасности
3.	Анализ мирового рынка антивирусного программного обеспечения
4.	Электронная цифровая подпись.
5.	Компьютерная преступность в России
6.	Модель угроз информации на территории РФ
7.	Алгоритмы цифровой подписи
8.	Способы защиты операционных систем
9.	Экономические основы защиты конфиденциальной информации
10.	Анализ мирового рынка антивирусного программного обеспечения
11.	Аудит безопасности корпоративных информационных систем
12.	Безопасность электронной почты и Интернет
13.	Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний
14.	Виды аудита информационной безопасности
15.	Выбор показателей защищенности от несанкционированного доступа к

	информации
16.	Государственная система защиты информации РФ
17.	Методы защиты аудио и визуальных документов
18.	Методы защиты документов на бумажных носителях
19.	Методы и средства обеспечения безопасности ПО
20.	Методы скрытой передачи информации
21.	Методы экономического анализа систем информационной безопасности
22.	Проблемы безопасности и пути их решения в современных компьютерных сетях
23.	Современные технологии архивирования данных
24.	Технологии резервного копирования данных
25.	Управление безопасностью приложений (на примере компании….)

Вопросы для самостоятельного изучения 8,9 семестр

№ п/п	Темы для самостоятельного изучения
1.	Проблемы безопасности в локальных сетях
2.	Технологии защиты Web-ресурсов от взлома и хакерских атак
3.	Проблемы безопасности в глобальных сетях
4.	Политика информационной безопасности в РФ
5.	Политика информационной безопасности в США
6.	Концепция электронного документа и проблемы правового регулирования электронно-цифровой подписи
7.	Стандарты шифрования
8.	Методы защиты речевой информации
9.	Виды компьютерных правонарушений.
10.	Методы защиты аудио и визуальных документов
11.	Методы защиты документов на бумажных носителях
12.	Методы внедрения программных закладок
13.	Методы защиты информации в Интернет.
14.	Методы защиты от макро-вирусов
15.	Методы защиты программ от несанкционированных изменений
16.	Методы защиты речевой информации
17.	Методы и средства борьбы со спамом
18.	Методы и средства обеспечения безопасности ПО
19.	Методы перехвата и навязывания информации
20.	Методы поиска и сбора информации.
21.	Методы скрытой передачи информации
22.	Методы экономического анализа систем информационной безопасности
23.	Методы защиты аудио и визуальных документов
24.	Методы защиты документов на бумажных носителях
25.	Методы внедрения программных закладок
26.	Методы защиты информации в Интернет.

Критерии оценки доклада (реферата):

– оценка «отлично» (8-10 баллов) выставляется студенту, если:

проведенное исследование и изложенный в докладе материал соответствует заданной теме;

представленные в докладе сведения отвечают требованиям актуальности и новизны;
продумана структура и стиль сопроводительной презентации;
студент способен ответить на вопросы преподавателя по теме доклада.

– оценка «хорошо» (4-7 баллов):
представленный в докладе материал соответствует заданной теме, однако присутствуют недостатки в связности изложения и структуре сопроводительной презентации;
не все выводы носят аргументированный и доказательный характер.

– оценка «удовлетворительно» (1-3 баллов):
студент способен изложить материал доклада, однако наблюдаются отклонения от заданной темы;
сопроводительная презентация подготовлена, но плохо соотносится с представленным докладом.

– оценка «неудовлетворительно» (0 баллов):
материал не соответствует заданной теме;
отсутствует сопроводительная презентация к докладу;
студент не освоил материал полностью и не способен ответить на вопросы преподавателя по теме доклада.

ТЕМЫ КУРСОВЫХ ПРОЕКТОВ ПО ДИСЦИПЛИНЕ
«Информационная безопасность»

№	**Темы курсовых проектов**
	Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками.
	Анализ методов и средств анализа защищенности беспроводных сетей.
	Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей.
	Разработка комплексной защиты информации на предприятии
	Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей
	Анализ средств защиты от спама.
	Разработка системы защиты персональных данных в предприятии
	Сравнительный анализ методов перехвата паролей пользователей компьютерных систем и методов противодействия им
	Анализ схем мошенничества в сети Интернет
	Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).
	Разработка мер по технической защите конфиденциальной информации в организации
	1. Анализ безопасности ОС Linux

	Сравнительный анализ средств защиты электронной почты
	Разработка комплексной системы защиты коммерческой информации
	Анализ внедрения технологий цифровой подписи в РФ
	Анализ возможности применения средств защиты информации на предприятиях
	Разработка системы управления кадровой безопасностью организации
	Разработка типового проекта защиты локальной вычислительной сети предприятия
	Разработка политики информационной безопасности.
	Анализ основных угроз электронного документооборота
	Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации
	Сравнительный анализ систем обнаружения атаки
	Сравнительный анализ программных средств, реализующих стеганографические методы защиты информации.
	Сравнительный анализ международных стандартов в области информационной безопасности и управления рисками
	Разработка системы информационной безопасности банка
	Сравнительный анализ способов информационного воздействия в сети Интернет
	Анализ современных средств анализа защищенности
	Сравнительный анализ методов аутентификации пользователей.
	Разработка мероприятий защиты персональных данных в организации.
	Анализ средств защиты компакт-дисков от несанкционированного копирования.
	Сравнительный анализ инструментальные средства анализа рисков информационной безопасности.
	Анализ основных угроз электронного документооборота - фундамент электронного бизнеса.

Приложение 1

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа №1
Разграничение прав пользователей в защищенных версиях операционной системы Windows

Цель работы: освоение средств администратора защищенных версий операционной системы Windows, предназначенных для

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

1) какие существуют способы аутентификации пользователей?
2) в чем слабость парольной аутентификации?
3) как может быть повышена надежность аутентификации с помощью паролей?
4) какой может быть реакция системы на попытку подбора паролей?
5) кому может быть разрешен доступ по чтению и по записи к базе учетных записей пользователей?
6) как должны храниться пароли в базе учетных записей пользователей?
7) в чем смысл объединения пользователей в группы?

Порядок выполнения работы:

1. Освоить средства регистрации пользователей:

- открыть список зарегистрированных пользователей (Панель управления | Администрирование | Управление компьютером | Локальные пользователи и группы | Пользователи);
- с помощью команды контекстного меню (Новый пользователь) создать для себя учетную запись с произвольным логическим именем, введя в качестве строки описания текст «Студент группы___)»);
- включить в отчет о лабораторной работе
  - ♦ копию экранной формы создания новой учетной записи,
  - ♦ копию экранной формы со списком зарегистрированных пользователей,
  - ♦ список команд контекстного меню (при отсутствии выделения имени пользователя в списке).
- выделить имя вновь зарегистрированного пользователя и с помощью команды контекстного меню (Свойства) просмотреть ее свойства;
- включить в отчет о лабораторной работе копию экранной формы со свойствами учетной записи на вкладке «Общие» и объяснение разницы между отключением и блокировкой учетной записи;
- включить в отчет о лабораторной работе копию экранной формы со свойствами учетной записи на вкладке «Членство в группах» и ответ на вопрос, в какую группу по умолчанию включается вновь созданный пользователь;
- с помощью кнопок «Добавить», «Дополнительно» и «Поиск» включить вновь созданного пользователя также в любую группу.
- включить в отчет о лабораторной работе копии экранных форм, используемых при добавлении пользователя в другую группу, и ответ на вопрос, как можно удалить пользователя из группы;

- включить в отчет о лабораторной работе список команд контекстного меню при выбранном имени учетной записи вместе с пояснениями их смысла, а также ответы на вопросы
  - ♦ когда должна применяться команда «Задать пароль»,
  - ♦ в чем опасность ее применения,
  - ♦ как должна происходить смена пароля пользователем.

3. Освоить средства работы с группами:

- открыть список групп (Панель управления | Администрирование | Управление компьютером | Локальные пользователи и группы | Группы);
- включить в отчет сведения об автоматически создаваемых группах пользователей, их именах и характеристиках прав их членов;
- создать новую группу в системе с именем «Начинающие пользователи» и включить в отчет о лабораторной работе копию используемого при этом экрана и сведения о порядке создания в системе новых групп пользователей, а также ответ на вопрос, в чем целесообразность разбиения множества пользователей на группы.

4. Освоить порядок назначения прав пользователям:

- открыть окно настройки прав пользователей (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя);
- исключить группу пользователей «Все» из числа групп, обладающих правом «Доступ к компьютеру из сети»;
- исключить пользователя «Гость» из числа пользователей, обладающих правом «Локальный вход в систему»;
- добавить группу «Начинающие пользователи» к списку пользователей, обладающих правом «Локальный вход в систему»;
- включить в отчет о лабораторной работе копии экранов, используемых при назначении прав пользователям, и сведения о порядке выполнения этих действий;
- с помощью раздела справки Windows «Назначение прав пользователя» включить в отчет о лабораторной работе пояснения отдельных привилегий пользователей системы (в соответствии с номером варианта и приложением 1). Обязательно ответить на вопрос, почему использование данного права должно быть ограничено.

5. Освоить определение параметров политики безопасности, относящихся к аутентификации и авторизации пользователей при интерактивном входе:

- открыть окно определения параметров безопасности для паролей (Панель управления | Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей);
- включить в отчет о лабораторной работе сведения о порядке назначения максимального и минимального сроков действия паролей и ответ на вопрос о смысле подобных ограничений;
- включить в отчет о лабораторной работе сведения о порядке назначения минимальной длины и ограничений на сложность паролей, а также ответы на вопросы, какие и почему требования по сложности предъявляются к паролям в операционной системе Windows (с помощью справочной подсистемы);
- включить в отчет о лабораторной работе сведения о назначении параметров «Требовать неповторяемости паролей» и «Хранить пароли всех пользователей в домене, используя обратимое шифрование» (с помощью справки Windows);
- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, относящихся к паролям;
- открыть окно определения параметров безопасности для политики блокировки учетных записей (Панель управления | Администрирование | Локальная политика

безопасности | Политики учетных записей | Политика блокировки учетных записей);

- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, и сведения о назначении этих параметров.

6. Включить в отчет по лабораторной работе ответы на контрольные вопросы:

- каковы основные цели угроз безопасности информации в компьютерных системах?
- насколько средства, изученные при выполнении лабораторной работы, могут нейтрализовать эти угрозы?
- каковы другие признаки, в соответствии с которыми может быть проведена классификация угроз безопасности в компьютерных системах?
- каковы основные каналы утечки конфиденциальной информации в компьютерных системах?
- насколько средства, изученные при выполнении лабораторной работы, могут перекрыть эти каналы?

7. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист с названиями университета, факультета, кафедры, учебной дисциплины и лабораторной работы, номером варианта, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы;
- ответы на контрольные вопросы.

Порядок защиты лабораторной работы:

1. К защите лабораторной работы допускаются студенты, выполнившие ее в компьютерном классе, предъявившие результаты своей работы преподавателю и подготовившие отчет о выполнении лабораторной работы.
2. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.
3. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая в при определении его итогового рейтинга за семестр.

Лабораторная работа №2

Реализация политики безопасности в защищенных версиях операционной системы Windows

Цель работы: освоения средств администратора и аудитора защищенных версий операционной системы Windows, предназначенных для

- определения параметров политики безопасности;
- определения параметров политики аудита;
- просмотра и очистки журнала аудита.

Подготовка к выполнению работы: по материалам лекций по дисциплине и изученным ранее дисциплинам вспомнить и подготовить для включения в отчет о лабораторной работе определения понятий

- *аудит*;
- *событие безопасности*;
- *журнал* (*файл*) *аудита*;
- *политика аудита*;
- *интерактивный вход*;
- *сетевой доступ*;
- *домен компьютерной сети*;
- *цифровая подпись*.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

1) какие события безопасности должны фиксироваться в журнале аудита?
2) какие параметры определяют политику аудита?
3) целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?
4) целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?
5) как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?
6) нужно ли ограничивать права пользователей по запуску прикладных программ и почему?

Порядок выполнения работы:

1. После собеседования с преподавателем и получения допуска к работе войти в систему под указанным именем (с правами администратора).
2. Освоить средства определения политики безопасности:

- открыть окно определения параметров политики безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности);
- установить заголовок «ПРЕДУПРЕЖДЕНИЕ» в качестве значения параметра «Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему»;
- установить текст «На этом компьютере могут работать только зарегистрированные пользователи!» в качестве значения параметра «Интерактивный вход в систему: текст сообщения для пользователей при входе в систему»;
- установить значение «Отключен» для параметра «Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL»;
- установить значение «Включен» для параметра «Интерактивный вход в систему: не отображать последнего имени пользователя»;
- установить значение «7 дней» для параметра «Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее»;
- включить в отчет о лабораторной работе сведения о порядке назначения параметров политики безопасности, относящихся к интерактивному входу, и ответ на вопрос о смысле этих параметров;

- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, относящихся к интерактивному входу;
- с помощью раздела Справки Windows «Параметры безопасности» включить в отчет о лабораторной работе пояснения отдельных параметров локальной политики безопасности компьютерной системы и их возможных значений (в соответствии с номером варианта и приложением 1). Обязательно ответить на вопрос, чем может угрожать неправильное определение данного параметра.

3. Освоить средства определение политики аудита:

- открыть окно определения параметров политики аудита (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Политика аудита);
- с помощью параметров политики аудита установить регистрацию в журнале аудита успешных и неудачных попыток
    - ♦ входа в систему,
    - ♦ изменения политики,
    - ♦ использования привилегий,
    - ♦ событий входа в систему,
    - ♦ управления учетными записями;
- открыть окно определения параметров безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности) и включить в отчет о лабораторной работе ответ на вопрос, какие еще параметры политики аудита могут быть определены;
- открыть окно просмотра журнала аудита событий безопасности (Панель управления | Просмотр событий | Безопасность), выполнить команду «Свойства» контекстного меню (или команду Действие | Свойства) и включить в отчет о лабораторной работе ответы на вопросы
    - ♦ какие еще параметры политики аудита могут быть изменены,
    - ♦ где расположен журнал аудита событий безопасности;
- включить в отчет о лабораторной работе сведения о порядке назначения параметров политики аудита и ответ на вопрос о смысле этих параметров;
- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики аудита.

4. Освоить средства просмотра журнала аудита событий безопасности:

- открыть окно просмотра журнала аудита событий безопасности (Панель управления | Просмотр событий | Безопасность);
- включить в отчет о лабораторной работе копии экранных форм с краткой и полной информацией о просматриваемом событии безопасности;
- с помощью буфера обмена Windows и соответствующей кнопки в окне свойств события включить в отчет о лабораторной работе полную информацию о нескольких событиях безопасности.

5. Освоить средства определения политики ограниченного использования программ:

- открыть окно определения уровней безопасности политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Уровни безопасности);
- включить в отчет о лабораторной работе пояснения к возможным уровням безопасности при запуске программ и копии соответствующих экранных форм;
- открыть окно определения дополнительных правил политики ограниченного использования программ (Панель управления | Администрирование | Локальная

политика безопасности | Политики ограниченного использования программ | Дополнительные правила);

- включить в отчет о лабораторной работе ответы на вопросы, какие дополнительные правила для работы с программами могут быть определены (с помощью команд контекстного меню или меню «Действие») и в чем их смысл, а также копии соответствующих экранных форм.

6. Включить в отчет о лабораторной работе ответы на контрольные вопросы:

- в чем уязвимость с точки зрения безопасности информации принимаемая по умолчанию реакция системы на превышение размера журнала аудита?
- какое из дополнительных правил ограниченного использования программ кажется Вам наиболее эффективным и почему?
- из каких этапов состоит построение политики безопасности для компьютерной системы?
- к чему может привести ошибочное определение политики безопасности (приведите примеры)?
- почему, на Ваш взгляд, многие системные администраторы пренебрегают использованием большинства из рассмотренных в данной лабораторной работе параметров политики безопасности?

7. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист с названиями университета, факультета, кафедры, учебной дисциплины и лабораторной работы, номером варианта, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы;
- ответы на контрольные вопросы.

Порядок защиты лабораторной работы:

4. К защите лабораторной работы допускаются студенты, выполнившие ее в компьютерном классе, предъявившие результаты своей работы преподавателю и подготовившие отчет о выполнении лабораторной работы, содержание которого соответствует п. 7 порядка выполнения работы;
5. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.
6. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая в при определении его итогового рейтинга за семестр.
7. В случае неудовлетворительной оценки по результатам защиты лабораторной работы или пропуска соответствующего занятия студент должен защитить работу повторно в другой день.

Лабораторная работа №3

Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

Цель работы: освоение средств защищенных версий операционной системы Windows, предназначенных для

- разграничения доступа субъектов к папкам и файлам;
- разграничения доступа субъектов к принтерам;
- разграничения доступа к разделам реестра;

- обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.

Подготовка к выполнению работы: по материалам лекций по дисциплине и изученным ранее дисциплинам вспомнить и подготовить для включения в отчет о лабораторной работе определения понятий

- дискреционная политика безопасности;
- мандатная политика безопасности;
- субъект доступа;
- объект доступа;
- виды доступа;
- монитор обращений;
- монитор безопасности объектов;
- домен безопасности;
- реестр операционной системы;
- контроль целостности объектов;
- ключ симметричного шифрования;
- ключи асимметричного шифрования.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

1) в чем достоинства и недостатки дискреционной политики безопасности?
2) в чем достоинства и недостатки мандатной политики безопасности?
3) в чем заключается тождественность объектов и тождественность субъектов компьютерной системы?
4) кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?
5) каковы возможные пути нарушения политики безопасности в компьютерной системе?
6) какие факторы влияют на определение размеров доменов безопасности?
7) какая информация хранится в реестре Windows?

Порядок выполнения работы:

1. После собеседования с преподавателем и получения допуска к работе войти в систему с указанным общим именем учетной записи (с правами обычного пользователя).
2. Освоить средства разграничения доступа пользователей к папкам:

- выполнить команду «Общий доступ и безопасность» контекстного меню папки, содержащей отчеты студентов о выполненных лабораторных работах (если эта команда недоступна, то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки) или команду «Свойства»;
- открыть вкладку «Безопасность» и включить в отчет сведения о субъектах, которым разрешен доступ к папке и о разрешенных для них видах доступа;
- с помощью кнопки «Дополнительно» открыть окно дополнительных параметров безопасности папки (вкладка «Разрешения»);
- включить в отчет сведения о полном наборе прав доступа к папке для каждого из имеющихся в списке субъектов;
- открыть вкладку «Владелец», включить в отчет сведения о владельце папки и о возможности его изменения обычным пользователем;
- открыть папку «Аудит», включить в отчет сведения о назначении параметров аудита, устанавливаемых на этой вкладке, и о возможности их установки обычным пользователем;
- закрыть окно дополнительных параметров безопасности и с помощью кнопки «Добавить» открыть окно выбора пользователя или группы;

• с помощью кнопок «Дополнительно» и «Поиск» открыть список зарегистрированных пользователей и групп и выбрать пользователя с именем своей индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
• назначить ему права на полный доступ к папке с отчетами о выполненных лабораторных работах;
• включить в отчет копии экранных форм, использованных при выполнении заданий данного пункта.

3. Освоить средства разграничения доступа пользователей к файлам:
• выполнить команду «Свойства» контекстного меню файла с одним из отчетов о ранее выполненных лабораторных работах;
• повторить все задания п. 2, но применительно не к папке, а к файлу;
• включить в отчет ответ на вопрос, в чем отличие определения прав на доступ к файлам по сравнению с определением прав на доступ к папкам.

4. Освоить средства разграничения доступа к принтерам:
• выполнить команду «Принтеры и факсы» меню «Пуск»;
• выполнить команду «Свойства» контекстного меню установленного в системе принтера;
• повторить все задания п. 2, но применительно не к папке, а к принтеру (кроме добавления нового субъекта к списку управления доступом);
• включить в отчет ответ на вопрос, в чем отличие определения прав на доступ к принтерам по сравнению с определением прав на доступ к папкам и файлам.

5. Освоить средства разграничения доступа к разделам реестра операционной системы:
• с помощью команды «Выполнить» меню «Пуск» запустить программу редактирования системного реестра regedit (regedt32);
• с помощью команды «Разрешения» меню «Правка» редактора реестра определить и включить в отчет сведения о правах доступа пользователей к корневым разделам реестра, их владельцах и параметрах политики аудита (аналогично п. 2);
• включить в отчет копии экранных форм, использованных при выполнении данного пункта, и ответ на вопрос, в чем отличие определения прав на доступ к разделам реестра по сравнению с определением прав на доступ к папкам и файлам.

6. Освоить средства обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы:
• выполнить команду «Свойства» контекстного меню папки, содержащей отчеты о ранее выполненных лабораторных работах, и на вкладке «Общие» окна свойств нажать кнопку «Другие»;
• включить выключатель «Шифровать содержимое для защиты данных», нажать кнопку «Применить» и в окне подтверждения изменения атрибутов нажать кнопку «Ok»;
• включить в отчет ответ на вопрос, как визуально выделяются имена зашифрованных файлов и папок;
• выполнить команду «Свойства» контекстного меню папки с отчетами о ранее выполненных лабораторных работах;
• нажать кнопку «Другие» и включить в отчет ответ на вопрос, доступна ли кнопка «Подробно»;
• повторить два предыдущих пункта для одного из файлов с отчетами о ранее выполненных лабораторных работах;

- выйти из системы и войти повторно под именем индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
- создать произвольный файл (например, с копией описания данной лабораторной работы) в папке «Мои документы» и обеспечить шифрование этого файла;
- выйти из системы и снова войти под именем общей учетной записи, под которой работали первоначально;
- выполнить команду «Свойства» контекстного меню одного из файлов с отчетами о ранее выполненных лабораторных работах, нажать последовательно кнопки «Другие» и «Подробно»;
- в окне подробностей шифрования нажать кнопку «Добавить» и в окне выбора пользователя выбрать имя индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
- повторить два предыдущих пункта для всех файлов с отчетами о ранее выполненных работах;
- снова выйти из системы и войти повторно под именем индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
- убедиться, что под индивидуальной учетной записью можно просматривать и редактировать отчеты о ранее выполненных лабораторных работах;
- включить в отчет копии экранных форм, использованных при выполнении данного пункта, сведения о порядке использования шифрующей файловой системы и ответы на вопросы
- как формируется список пользователей, из которого возможен выбор субъектов для совместного доступа к зашифрованным файлам;
- связан ли этот список с зарегистрированными в системе пользователями и группами;
- каковы функции агента восстановления зашифрованных файлов и как он может быть назначен (воспользуйтесь Справкой Windows).

7. Ознакомиться с правами доступа к файлам и папкам, назначаемым операционной системой по умолчанию:
- выполнить команду «Общий доступ и безопасность» (команду «Свойства») контекстного меню одной из папок с документами зарегистрированного в системе пользователя (например, «Документы - Пользователь компьютерного класса») и открыть вкладку «Безопасность»;
- включить в отчет сведения о правах доступа пользователей к данной папке и о ее владельце;
- повторить два предыдущих пункта для папки с документами другого зарегистрированного пользователя;
- повторить два предыдущих пункта для папки «Общие документы»;
- включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта, и ответы на вопросы
- как обеспечивается операционной системой разграничение доступа к личным документам пользователей (по умолчанию);
- где (по умолчанию) должны находиться документы, предназначенные для совместного использования.

8. Включить в отчет о лабораторной работе ответы на контрольные вопросы:
- какая политика безопасности лежит в основе разграничения доступа к объектам в защищенных версиях операционной системы Windows?
- в чем уязвимость принятой в защищенных версиях операционной системы Windows политики разграничения доступа (приведите примеры)?

- как работает механизм наследования при определении прав на доступ субъектов к объектам в защищенных версиях операционной системы Windows?
- какие дополнительные возможности разграничения доступа к информационным ресурсам предоставляет шифрующая файловая система?
- насколько, на Ваш взгляд, удобно использование шифрующей файловой системы (в том числе при необходимости совместной работы над документами)?
- какой стандартный механизм работы с личными и общими документами предлагается в защищенных версиях операционной системы Windows и насколько, на Ваш взгляд, он удобен?

9. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист с названиями, факультета, кафедры, учебной дисциплины и лабораторной работы, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы;
- ответы на контрольные вопросы.

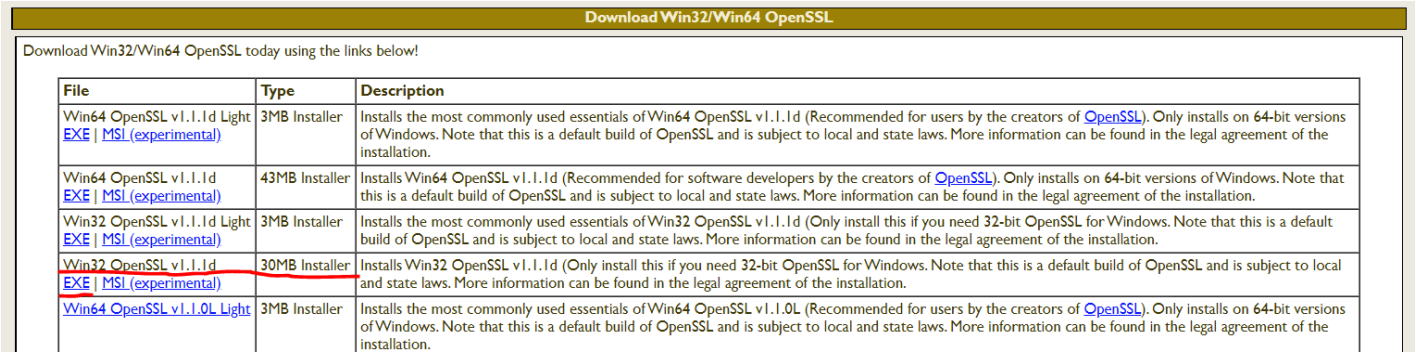
Порядок защиты лабораторной работы:

1. К защите лабораторной работы допускаются студенты, выполнившие ее в компьютерном классе, предъявившие результаты своей работы преподавателю и подготовившие отчет о выполнении лабораторной работы, содержание которого соответствует п. 9 порядка выполнения работы;
2. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.
3. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая в при определении его итогового рейтинга за семестр.
4. В случае неудовлетворительной оценки по результатам защиты лабораторной работы или пропуска соответствующего занятия студент должен защитить работу повторно в другой день.

Лабораторная работа №4.

Создание самоподписанных сертификатов.

1. Расписать: Описание SSL-сертификатов, для чего они применяются, каких видов бывают. Описание .pem, .crt, .cer, .key, .csr ключей.
2. Найти в сети Интернет 3 ресурса для покупки Wildcard SSL-сертификатов с наиболее низкой ценой. В отчет внести скриншоты с указанием цен.
3. Скачать и установить полную 32-битную или 64-битную версию OpenSSL (EXE) в зависимости от разрядности вашей ОС.
   Ссылка на скачивание https://slproweb.com/products/Win32OpenSSL.html

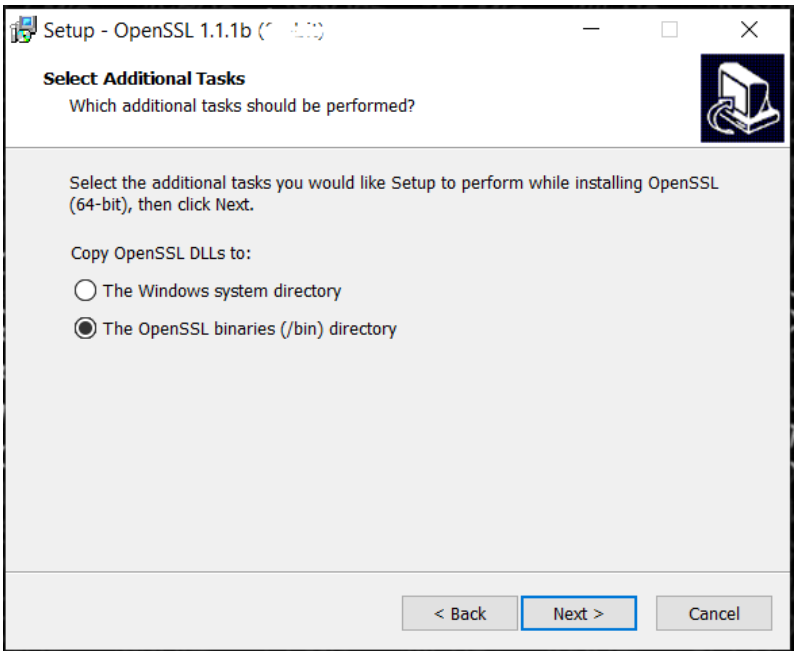


Download Win32/Win64 OpenSSL

Download Win32/Win64 OpenSSL today using the links below!

File	Type	Description
Win64 OpenSSL v1.1.1d Light EXE | MSI (experimental)	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.1d (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.1d EXE | MSI (experimental)	43MB Installer	Installs Win64 OpenSSL v1.1.1d (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1d Light EXE | MSI (experimental)	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.1d (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1d EXE | MSI (experimental)	30MB Installer	Installs Win32 OpenSSL v1.1.1d (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0L Light	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.0L (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

При установке на пункте выбора места копирования DLL-файлов, ОБЯЗАТЕЛЬНО выбрать директорию /bin



Запустить программу openssl.exe от имени администратора из папки C:\Program Files\OpenSSL-Win32\bin (в 64-битной версии возможно расположение C:\Program Files (x86)\OpenSSL-Win32\bin).

4. Создать самоподписанный сертификат следуя инструкциям. В отчет внести скриншоты по каждому выполняемому шагу. В наименовании файлов вместо “domain” использовать вашу фамилию латинскими буквами.

Создание закрытого ключа и запроса на подпись.

Чтобы создать закрытый ключ и запрос на подпись открытого ключа выполните такую команду:

```
req -newkey rsa:2048 -nodes -keyout domain.key -out domain.csr
```

После чего необходимо указать следующие сведения на латинице:

- *2х буквенное обозначение страны*
- *Республику*
- *Населенный пункт*
- *Название организации – Свою фамилию*
- *Отдел – IT*
- *Доменное имя, вида «имя».ru*
- *Свой email*
- *Указать какой-либо пароль*
- *Дополнительно название компании – Свое имя.*

```
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Chechen Republic
Locality Name (eg, city) []:Grozny
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Zaurbekov
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:rizvan.ru
Email Address []:rizvan@mail.ru

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345678
An optional company name []:Rizvan
OpenSSL>
```

Подпись сертификатов.

Выполните команду для подписания сертификата сроком 365 дней:

```
x509 -signkey domain.key -in domain.csr -req -days 365 -out domain.crt
```

Внести в отчет скриншот содержания папки C:\Program Files\OpenSSL-Win32\bin , где по умолчанию создаются ключи.

Внести в отчет скриншоты всех вкладок созданного сертификата.

Внести в отчет скриншоты содержания файлов закрытого ключа и файла запроса, открыв с помощью текстового редактора.

Просмотр файла запроса, сертификата и закрытого ключа с помощью OpenSSL. Поэтапно ввести 3 команды и внести в отчет результаты каждой из них.

```
req -text -noout -verify -in domain.csr

x509 -text -noout -in domain.crt

rsa -check -in domain.key
```

Лабораторная работа №5. Использование электронных идентификаторов Рутокен и JaCarta.

Использование криптографических средств защиты информации КриптоПро CSP и VipNet CSP.

1. Электронные идентификаторы Рутокен и JaCarta. Описание, возможности, примеры использования.
2. СКЗИ КриптоПро CSP и VipNet CSP. Описание, возможности, примеры использования. Основные отличия.
3. Скачать и установить СКЗИ КриптоПро CSP и VipNet CSP с официальных источников - https://www.cryptopro.ru/ , https://infotecs.ru/

Включить в отчет скриншоты регистрации на сайте производителя, хода установки ПО, а также всех вкладок и настроек установленного ПО.

Лабораторная работа №6.
Шифрование данных. Использование ПО КриптоАРМ.

1. ПО КриптоАРМ. Описание, возможности, примеры использования.

В отчет включить скриншоты всех дальнейших действий.

2. Скачать КриптоАРМ 4 с официального сайта производителя https://www.trusted.ru/
3. Установить ПО. Во время установки выбрать «КриптоАРМ Старт» и Полная установка:
4. Запустить установленное ПО.
5. Зайти в раздел «Сертификаты» и создать самоподписанный сертификат используя вашу фамилию в поле «Идентификатор (CN)».
6. Создать документ, используя вашу фамилию в наименовании. Ввести в документе произвольный текст.
7. С помощью ПО КриптоАРМ подписать созданный документ, используя созданный самоподписанный сертификат.
8. Аналогично провести процедуры «Шифрование» и «Подписание и шифрование», используя собственный сертификат.
9. Включить в отчет скриншоты полученных зашифрованных файлов и описать расширения данных файлов.
10. Произвести процедуру расшифрования зашифрованного документа и сохранить его с другим наименованием. Проверить содержание документа.

Приложение 2

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ К РУБЕЖНОМУ КОНТРОЛЮ

Первая рубежная аттестация (7 –й семестр)

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 1

1. Введение в информационную безопасность
2. Задачи и методы информационной безопасности

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровойэкономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 2

1. Угрозы информационной безопасности
2. Потенциальные противники и атаки

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 3

1. Введение в информационную безопасность
2. Организационно-правовые методы информационной безопасности

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 4

1. Задачи и методы информационной безопасности
2. Потенциальные противники и атаки

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт _цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 5

1. Угрозы информационной безопасности
2. Потенциальные противники и атаки

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт _цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 6

1. Организационно-правовые методы информационной безопасности
2. Потенциальные противники и атаки

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт _цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 7

1. Стандарты обеспечения ИБ
2. Потенциальные противники и атаки

Подпись преподавателя _____ Подпись заведующего кафедрой_____

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ К РУБЕЖНОМУ КОНТРОЛЮ

Вторая рубежная аттестация (7 –й семестр)

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 1

1. Законодательный уровень информационной безопасности
2. Основные положения теории информационной безопасности информационных систем

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровойэкономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 2
Подпись преподавателя _____ Подпись заведующего кафедрой _____

1. Административный уровень информационной безопасности
2. Основные положения теории информационной безопасности информационных систем

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 3

1. Основные технологии построения защищенных экономических информационных систем.
2. Модель угроз информации на территории РФ

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 4

1. Модель угроз информации на территории РФ
2. Способы защиты операционных систем

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт _цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 5

1. Способы защиты операционных систем
2. Анализ мирового рынка антивирусного программного обеспечения

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт _цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 6

1. Анализ мирового рынка антивирусного программного обеспечения
2. Компьютерная преступность в России

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт _цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «7»
Дисциплина «Информационная безопасность»
Билет № 7

1. Модель угроз информации на территории РФ
2. Анализ мирового рынка антивирусного программного обеспечения

Подпись преподавателя _____ Подпись заведующего кафедрой _____

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ К РУБЕЖНОМУ КОНТРОЛЮ

Первая рубежная аттестация (8 –й семестр)

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 1

1. Управление рисками
2. Процедурный уровень информационной безопасности

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровойэкономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 2

1. Управление рисками
2. Программно-технические методы защиты

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 3

1. Процедурный уровень информационной безопасности
2. Идентификация и аутентификация

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 4

1. Программно-технические методы защиты
2. Сервисы управления доступом

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт _цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 5

1. Процедурный уровень информационной безопасности
2. Сервисы управления доступом

Подпись преподавателя _____ Подпись заведующего кафедрой _____

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ К РУБЕЖНОМУ КОНТРОЛЮ

Вторая рубежная аттестация (8 –й семестр)

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 1

1. Протоколирование и аудит
2. Экранирование и анализ защищенности

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. Акад. М.Д. Миллионщикова
Институт цифровойэкономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 2
Подпись преподавателя _____ Подпись заведующего кафедрой _____

1. Тунелирование и управление
2. Протоколирование и аудит

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 3

1. Экранирование и анализ защищенности
2. Обеспечение высокой доступности

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 4

1. Обеспечение высокой доступности
2. Криптографические методы защиты

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт _цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 5

1. Обеспечение высокой доступности
2. Протоколирование и аудит

Подпись преподавателя _____ Подпись заведующего кафедрой _____

Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Институт _цифровой экономики и технологического предпринимательства
Группа «БИН-» Семестр «8»
Дисциплина «Информационная безопасность»
Билет № 6

1. Экранирование и анализ защищенности
2. Криптографические методы защиты

Подпись преподавателя _____ Подпись заведующего кафедрой _____

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ К ЗАЧЕТУ (7-й семестр)

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 1

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__7__семестр

1. Введение в информационную безопасность

2. Задачи и методы информационной безопасности

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 2

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__7 семестр

1. Задачи и методы информационной безопасности

2. Угрозы информационной безопасности

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 3

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__7__семестр

1. Угрозы информационной безопасности

2. Потенциальные противники и атаки

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 4

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__7__семестр

1. Законодательный уровень информационной безопасности

2. Основные положения теории информационной безопасности информационных систем

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 5

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__7__семестр

1. Основные технологии построения защищенных экономических информационных систем

2. Модель угроз информации на территории РФ

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 6

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__7__семестр

1. Способы защиты операционных систем

2. Анализ мирового рынка антивирусного программного обеспечения

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 7

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__8__семестр

1. Компьютерная преступность в России

2. Административный уровень информационной безопасности

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ К Экзамену (8-й семестр)

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 1

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__8__семестр

1. Управление рисками

2. Экранирование и анализ защищенности

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 2

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__8__семестр

1. Процедурный уровень информационной безопасности
2. Протоколирование и аудит

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 3

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__8__семестр

1. Программно-технические методы защиты
2. Криптографические методы защиты

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 4

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН-__8__семестр

1. Идентификация и аутентификация
2. Обеспечение высокой доступности

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 5

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _БИН- 8 __семестр

1. Сервисы управления доступом

2. Тунелирование и управление

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева