Приложение к ОПОП
«Организация и программирование интеллектуальных систем»

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
**«Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)**

РАБОЧАЯ ПРОГРАММА

дисциплины

«ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

для подготовки бакалавров

по направлению

09.03.01 «Информатика и вычислительная техника»

по профилю

«Организация и программирование интеллектуальных систем»

Санкт-Петербург

2024

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

доцент, к.т.н., доцент Горячев А.В.

Рабочая программа рассмотрена и одобрена на заседании кафедры ИБ 17.01.2024, протокол № 1

Рабочая программа рассмотрена и одобрена учебно-методической комиссией ФКТИ, 24.01.2024, протокол № 1

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	ФКТИ
Обеспечивающая кафедра	ИБ
Общая трудоемкость (ЗЕТ)	4
Курс	4
Семестр	7
Виды занятий	
Лекции (академ. часов)	34
Лабораторные занятия (академ. часов)	17
Практические занятия (академ. часов)	17
Иная контактная работа (академ. часов)	1
Все контактные часы (академ. часов)	69
Самостоятельная работа, включая часы на контроль (академ. часов)	75
Всего (академ. часов)	144
Вид промежуточной аттестации	
Экзамен (курс)	4

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Дисциплина «Защита компьютерной информации» обеспечивает теоретическую и практическую подготовку в области принципов, методов и средств защиты компьютерной информации от целенаправленных атак и непреднамеренных модификаций. Программа дисциплины включает в себя изучение основных видов угроз и атак, методов обнаружения вторжений и защиты от них, базовых инструментов информационной защиты. Особое внимание в курсе уделено знакомству с базовыми средствами информационной защиты. Лекционный материал дисциплины по каждому разделу подкрепляется примерами использования конкретных инструментов защиты и организационных мероприятий.

SUBJECT SUMMARY

«ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

The discipline ”computer information protection” provides theoretical and practical training of principles, methods and means protecting computer information from targeted attacks and unintentional modifications. The discipline program includes the study of the main types of threats and attacks, methods of intrusion detection and protection against them, basic information security tools. Special attention in the course is paid to familiarization with basic information security tools. The lecture material of the discipline for each section is supported by examples of the use of specific protection tools and organizational measures.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Целью изучения дисциплины является получение базовых знаний об информационной безопасности, основах формирования защищенной корпоративной сетевой среды, выработка умений настраивать параметры безопасности операционных систем и приложений, а также приобретение навыков применять знания об основах информационной безопасности при эксплуатации и формировании инфраструктуры безопасности корпоративной сети. Теоретический базис дисциплины основывается на знаниях из дискретной математики, теории кодирования, теории алгоритмов.

2. Задачей дисциплины является развитие навыков использования стандартных программных, технических и организационных средств обеспечения защиты корпоративной информации, навыков их настройки и умений быстро реагировать на экстренные ситуации.

3. Дисциплина обеспечивает приобретение знаний:
-об основных угрозах компьютерной информации;
-о принципах организации защиты корпоративной и персональной компьютерной информации;
-о проектировании инфраструктуры информационной безопасности;
-об основных методах организации информационных атак и способах их реализации.

4. Дисциплина формирует умения:
-организовывать защиту корпоративной информации;
-применять знания в области информационной безопасности при проектировании информационных систем.

5. Дисциплина развивает навыки использования стандартных программных,

технических и организационных средств обеспечения защиты корпоративной информации.

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Информатика»

2. «Объектно-ориентированное программирование»

3. «Организация ЭВМ и систем»

4. «Основы программирования на языке Ассемблера»

5. «Основы тестирования программного обеспечения»

6. «Операционные системы»

7. «Тестирование программного обеспечения»

8. «Математическая логика и теория алгоритмов»

9. «Межличностные коммуникации в малых группах и организациях»

10. «Правовые основы профессиональной деятельности и защиты прав на объекты интеллектуальной собственности»

11. «Производственная практика (технологическая (проектно-технологическая) практика)»

12. «Сети ЭВМ»

и обеспечивает изучение последующих дисциплин:

1. «Производственная практика (научно-исследовательская работа)»

2. «Производственная практика (преддипломная практика)»

3.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	**Наименование компетенции/индикатора компетенции**
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
ОПК-3.1	*Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности*
ОПК-3.3	*Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности*

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Лек, ач	Пр, ач	Лаб, ач	ИКР, ач	СР, ач
1	Введение	2				
2	Введение в защиту компьютерной информации. Модель эшелонированной обороны	2			1	5
3	Списки контроля доступа	2		2		4
4	Аутентификация. Службы каталогов сетевых ресурсов. Active Directory	2		2		5
5	Групповые политики Active Directory	2		2		5
6	Криптография с открытым и закрытым ключами. Сертификатфы. PKI	2		2		5
7	Шифрующая файловая система	2		2		4
8	Обеспечения высокого уровня доступности информации при хранении	2		2		5
9	Защита информации при обработке	2	2			4
10	Защита при передаче информации. Маршрутизация. SSL. IPSecurity	2		2		5
11	Удаленный доступ к ресурсам сети. VPN	2	1	1		4
12	Контроль за доступом к корпоративной сети. NIDS, NAP	2	2			5
13	Контроль за доступом к внешней среде. Межсетевые экраны. Технологии NAT, пакетной и контентной фильтрации, Proxy. Публикация информации. Демилитаризованная зона.	2	2	2		4
14	Виртуальные машины. Безопасность облачных технологий	2	2			4
15	Безопасность взаимодействия с Web	2	2			4
16	Атаки. Угрозы. Хакеры	1	2			4
17	Социальная инженерия. Корпоративные политики и правила	1	2			4
18	Работа с персональными данными. Законодательство в области ИБ	2	2			4
	Итого, ач	34	17	17	1	75
	Из них ач на контроль	0	0	0	0	35
	Общая трудоемкость освоения, ач/зе	144/4				

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Введение	Актуальность вопросов защиты компьютерной информации и структура курса
2	Введение в защиту компьютерной информации. Модель эшелонированной обороны	Определение компьютерной информации. Основные понятия защиты компьютерной информации. Модели компьютерной безопасности. Модель эшелонированной обороны. Уровни и подуровни модели. Классификация стандартных инструментов защиты информации
3	Списки контроля доступа	Управление доступом с помощью списков контроля доступом (ACL). Аутентификация и Авторизация. Понятие идентификатора безопасности (SID). Маркер доступа. Принципалы безопасности. Группы безопасности. Состав списка контроля доступа. Упрощенное и детальное представление ACL. Наследование ACL. Статическое и динамическое наследование. Блокирование наследования. Разрешение и запрет выполнения операции. Определение эффективных разрешений. Управление списком контроля доступа. Полномочия владельца объекта. Управление владением. Поведение ACL при копировании и переносе объекта. Формирование недоступных областей и их устранение.
4	Аутентификация. Службы каталогов сетевых ресурсов. Active Directory	Роль аутентификации в управлении доступом к ресурсам. Хранилища учетных данных. Отношения доверия. Прототипы: домен Windows NT. Лес Active Directory. Домен Active Directory. Подразделения. Доверительные отношения в лесу Active Directory. Контроллер домена. Роль контроллера домена при аутентификации. Хранилище данных Active Directory. Сайты Active Directory. Учетные записи пользователей. Процесс входа в систему в домене. Процесс доступа к сетевым ресурсам. Использование групп для контроля до-ступа на основе ролей. Области применения групп. Вложенность групп. Типы групп. Учетные записи компьютеров. Доверительные отношения между лесами.

№ п/п	Наименование темы дисциплины	Содержание
5	Групповые политики Active Directory	Концепция политики. Локальные политики безопасности. Шаблоны безопасности. Анализ и конфигурация безопасности. Понятие групповой политики Active Directory. Объекты групповой политики. Хранение объектов групповой политики. Административные шаблоны. Клиент групповой политики и его расширители. Применение политик разными операционными системами. Расширение функционала с помощью административных шаблонов. Порядок применения объектов групповой политики. Блокирование наследования. Область применения групповых политик. Обновление групповых политик. Предпочтения. Нацеливание предпочтений. Устранение конфликтов. Обработка групповых политик при медленном соединении.
6	Криптография с открытым и закрытым ключами. Сертификатфы. PKI	Формирование сертификата. Сертификат. Типы центров выдачи сертификатов. Атрибуты сертификата. Управление центром выдачи сертификатов. Шаблоны сертификатов. Жизненный цикл сертификата. Отзыв сертификата. Запрос сертификата через Web. Установка сертификата. Список доверенных сертификатов. Список отозванных сертификатов
7	Шифрующая файловая система	Проблемы списков контроля доступа. Концепция шифрования отдельных файлов. Получение самоподписанного сертификата. Совместное использование зашифрованного файла. Получение сертификата от центра выдачи сертификатов. Восстановление доступа к зашифрованным файлам при потере закрытого ключа. Агент восстановления шифрующей файловой системы. Копирование и перенос зашифрованных файлов. Управление разрешением на шифрование.
8	Обеспечения высокого уровня доступности информации при хранении	Резервное копирование. Схемы и правила резервного копирования. Обеспечение доступности при аппаратных проблемах в дисковой подсистеме. Дисковые массивы. Избыточные массивы независимых дисков (RAID). Зеркальные диски (RAID 1). Чередующиеся массивы с избыточностью (RAID 5). Другие способы повышения надежности дисковых массивов. Теневые копии. Механизм предыдущих копий. Кластеры надежности. Кворум. Перенос и восстановление узла кластера.
9	Защита информации при обработке	Защита хоста. Защита операционной системы. Аутентификация. Обеспечение целостности операционной системы. Автоматизация обновлений. Контроль за отсутствием закладок и появлением нецелевого кода. Программно-аппаратные решения. Антивирусы. Antimalware. Борьба с RootKit. Защита приложений. Службы обнаружения и предотвращения вторжений на хост (HIDS и HIPS). Аудит информационных систем.

№ п/п	Наименование темы дисциплины	Содержание
10	Защита при передаче информации. Маршрутизация. SSL. IPSecurity	Задачи защиты информации при переда-че. Защита трафика при взаимодействии с Web. Технология уровня приложений -SSL. Защита сетевой инфраструктуры сетевого уровня – IPSecurity. Возможности IPSecurity. Настройка взаимодействия IPSecurity в среде автономных компьютеров. Настройка IPSecurity в доменной среде. Детализированная настройка IPSecurity. Мониторинг соединений IPSecurity с помощью анализатора сетевых пакетов. Монитор IPSecurity.
11	Удаленный доступ к ресурсам сети. VPN	Концепция удаленного доступа к ресурсам сети. Механизмы удаленного доступа. Виртуальные частные сети (VPN). Концепция. Маршрутизация VPN. Протоколы VPN. Аутентификация в VPN. Инфраструктура удаленной аутентификации RADUIS. Управление серверами VPN в среде Active Directory. Автоматизация установки и настройки клиентов VPN. Корпоративный посредник сервиса VPN. Особенности IPv6. Механизм Direct Access
12	Контроль за доступом к корпоративной сети. NIDS, NAP	Принципы контроля за доступом к корпоративной сетевой среде. Сетевые сервисы обнаружения и предотвращения вторжений NIDS и NIPS. Управление доступом к корпоративной среде с контролем состояния компьютерной среды. Технология карантина. Способы реализации карантина при различных механизмах подключения к корпоративной среде. Инструменты управления доступом к сетевой среде NAC и NAP. Управление NAC в корпоративной среде на основе Windows.
13	Контроль за доступом к внешней среде. Межсетевые экраны. Технологии NAT, пакетной и контентной фильтрации, Proxy. Публикация информации. Демилитаризованная зона.	Понятие периметра сети. Демилитаризованная зона. Межсетевые экраны. Топология межсетевых экранов. Компоненты межсетевого экрана. Технология NAT – взаимодействие с Интернет из сети с приватной адресацией. Пакетная и контентная фильтрация. Технология Proxy. Публикация информации. Управление публикацией.
14	Виртуальные машины. Безопасность облачных технологий	Особенности работы операционных систем на виртуальных машинах. Управление доступом к виртуальным машинам. Особенности сетевого взаимодействия виртуальных машин. Защита сетевого взаимодействия. Общие проблемы безопасности облачных технологий. Особенности защиты коммуникаций с Azure.
15	Безопасность взаимодействия с Web	Основные особенности взаимодействия через Web. Средства защиты операционной системы. Встроенные механизмы обеспечения информационной безопасности обозревателей Интернет. Защита других сервисов глобального взаимодействия.

№ п/п	Наименование темы дисциплины	Содержание
16	Атаки. Угрозы. Хакеры	Кто такие хакеры. История хакерства. Виды атак. Причины выполнения атак. Угрозы. Модель угроз STRIDE. Жизненный цикл атаки. Защита от атак. Признаки атаки.
17	Социальная инженерия. Корпоративные политики и правила	Организационное обеспечение корпоративной информационной системы. Методы социальной инженерии. Основные принципы защиты от атак социальной инженерии. Управление социальными аспектами информационной системы. Корпоративные политики. Аппаратно-поддерживаемые политики. Методы реализации корпоративных политик – корпоративные правила.
18	Работа с персональными данными. Законодательство в области ИБ	Понятие персональных данных. Законодательство в области работы с персональными данными. Законодательства в области использования криптографических средств.

4.2 Перечень лабораторных работ

Наименование лабораторной работы	Количество ауд. часов
1. Списки контроля доступа	2
2. Аутентификация. Служба каталога сетевых ресурсов Active Directory	2
3. Групповые политики Active Directory	2
4. Сертификаты. PKI	2
5. Шифрующая файловая система EFS	2
6. Обеспечение высокого уровня доступности при хранении	2
7. SSL. IPSecurity	2
8. Удаленный доступ к ресурсам сети. VPN	1
9. Windows Firewall с расширенными возможностями	2
Итого	17

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. Защита информации при обработке. Антивирусы. Обновления.	2
2. Контроль за доступом к корпоративной сети. NIDS, NAP	2
3. Методы доступа к внешней среде. NAT. Proxy.	2
4. Виртуальные машины. Безопасность облачных технологий	2
5. Безопасность взаимодействия с Web	2
6. Удаленный доступ к ресурсам сети. VPN	1
7. Атаки. Угрозы. Хаккеры	2
8. Социальная инженерия. Корпоративные политики и правила	2

Наименование практических занятий	Количество ауд. часов
9. Работа с персональными данными. Законодательство в области ИБ	2
Итого	17

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

Индивидуальное домашнее задание не предусмотрено.

4.7 Доклад

Доклад не предусмотрен.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными литературными источниками и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников

материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины.

Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

Текущая СРС	**Примерная трудоемкость, ач**
Работа с лекционным материалом, с учебной литературой	15
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	0
Самостоятельное изучение разделов дисциплины	10
Выполнение домашних заданий, домашних контрольных работ	0
Подготовка к лабораторным работам, к практическим и семинарским занятиям	11
Подготовка к контрольным работам, коллоквиумам	4
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	0
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	0
Подготовка к зачету, дифференцированному зачету, экзамену	35
ИТОГО СРС	75

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Малюк А.А. Защита информации в информационном обществе. Учебное пособие для вузов / А.А. Малюк, 2015. -230 с. -Текст : электронный.	неогр.
2	Основы компьютерной безопасности : метод. указания к лаб. работам / Санкт-Петербургский государственный электротехнический университет им. В.И. Ульянова (Ленина) ”ЛЭТИ”, 2009. -1 эл. опт. диск (CD-ROM)	неогр.
3	Горячев, Александр Вадимович. Основы информационной безопасности распределенных САПР : учеб. пособие / А. В. Горячев, Н. Е. Новакова, 2015. -1 эл. опт. диск (CD-ROM). -Текст : электронный.	неогр.
4	Васильева, Екатерина Николаевна. Угрозы безопасности информационных технологий : учеб. пособие / Е.Н. Васильева, В.В. Цехановский, 2005. -63 с.	неогр.
5	Внуков, Андрей Анатольевич. Основы информационной безопасности: защита информации : учебное пособие для спо / А. А. Внуков., 2023. -161 с. -Текст : электронный.	неогр.
Дополнительная литература		
1	Информационная безопасность и защита информации : учеб. пособие для вузов по направлению ”Информац. системы и технологии” / Ю. Ю. Громов [и др.], 2015. -383 с.	14
2	Прохорова, Ольга Витольдовна. Информационная безопасность и защита информации : учеб. / О. В. Прохорова, 2020. -121 с.	39

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	Сайт ФСТЭК Россииhttp://fstec.ru
2	Нормативные и методические документы по технической защите информацииhttp://detektor.ru/about/regulations/organizacionno-rasporyaditel_nye_dokumenty_po_tehnicheskoj_zawite_informacii1/

5.3 Адрес сайта курса

Адрес сайта курса: https://vec.etu.ru/moodle/course/view.php?id=21810

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Защита компьютерной информации» предусмотрены следующие формы промежуточной аттестации: экзамен.

Экзамен

Оценка	Описание
Неудовлетворительно	Курс не освоен. Студент испытывает серьезные трудности при ответе на ключевые вопросы дисциплины
Удовлетворительно	Студент в целом овладел курсом, но некоторые разделы освоены на уровне определений и формулировок
Хорошо	Студент овладел курсом, но в отдельных вопросах испытывает затруднения. Умеет решать задачи
Отлично	Студент демонстрирует полное овладение курсом, способен применять полученные знания при решении конкретных задач

Особенности допуска

К экзамену допускаются студенты, выполнившие и защитившие в ходе семестра (до начала зачетной недели) не менее 6 лабораторных работ на коллоквиумах, а также сдавшие итоговый тест с оценкой не ниже 50% от максимальной.

Экзамен проводится по билетам. Критерии оценивания представлены выше.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Вопросы к экзамену

№ п/п	Описание
1	Модель эшелонированной обороны
2	Списки контроля доступа
3	Локальная аутентификация
4	Аутентификация в Active Directory
5	Управление конфигурацией компьютеров с помощью групповых политик Active Directory
6	Криптография с симметричным ключом. Примеры алгоритмов
7	Криптография с открытым и закрытым ключами. Примеры использования
8	Сертификаты. PKI
9	Шифрующая файловая система
10	Обеспечение высокого уровня доступности при хранении. Защита ”от дурака”
11	Обеспечение высокого уровня доступности при хранении. Защита от аппаратно-программных проблем
12	Защита информации при обработке. Методы изоляции процессов.
13	Защита информации при обработке. Антивирусы. Обновления.
14	Защита информации при передаче. Маршрутизация. SSL
15	Защита информации при передаче. IPSecurity
16	VPN
17	Контроль за доступом к корпоративной сети. NIDS. NAP
18	Выход в Интернет из корпоративной сети. Маршрутизация. Статический NAT.
19	Выход в Интернет из корпоративной сети. Динамический NAT
20	Выход в Интернет из корпоративной сети. Proxy
21	Межсетевой экран. Демилитаризованная зона.
22	Безопасность виртуальных машин и облачных технологий.
23	Безопасность взаимодействие с Web
24	Атаки. Угрозы. Хакеры
25	Социальная инженерия

26	Работа с персональными данными
27	Корпоративные политики и правила

Форма билета

Министерство науки и высшего образования Российской Федерации

ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина)»

_____

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

Дисциплина **Защита компьютерной информации** ФКТИ

1. Модель эшелонированной обороны

2. Выход в Интернет с помощью NAT

3. Задача

УТВЕРЖДАЮ

Заведующий кафедрой Е.Г. Воробьев

Образцы задач (заданий) для контрольных (проверочных) работ

Пример компьютерного теста:

1. Какие два уровня модели эшелонированной обороны имеют подуровни?

- Хранение
- **Обработка**
- **Передача**
- Физический доступ

2. Если пользователь получает на файл разрешение на какую-то операцию, а группа, в которую он входит, получает запрет на ту же операцию, то ка-

ков будет конечный результат? Выберите все верные ответы.

- **Запрет, если оба разрешения явные**
- Разрешено, если разрешение унаследовано
- Разрешено, только владельцу
- Запрещено всем
- Запрет, если разрешение унаследовано
- **Разрешение, если запрет унаследован**

3. Если пользователь получает на файл разрешение на какую-то операцию, а группа, в которую он входит, получает запрет на ту же операцию, то каков будет конечный результат.

- **Операция пользователю запрещена**
- Операция разрешена тем, у кого есть полный доступ к каталогу, где находится файл
- Операция разрешена только владельцу
- Если оба назначения сделаны на один и тот же объект, то операция запрещена, если – нет, то выигрывает то назначение, которое сделано на ближайший объект, прежде всего – на сам файл

4. Почему при задании прав доступа в дополнительных разрешениях вы можете увидеть запись разрешения через слэш (”Создание файлов / Запись данных”)?

- **При назначении этого разрешения к папке применяется разрешение на операцию, описанную до слэша, а к файлу, если он унаследует такое разрешение, будет применено разрешение на операцию, описанную после**
- Если назначение получено напрямую, то работает первая половина записи, если унаследована - то вторая
- Применение зависит от установленного атрибута отключения наследования

5. Если пользователь аутентифицировался в домене, то….

- **он может обратиться к любому домену леса без дополнительной аутентификации**
- В другом домене леса ему опять придется аутентифицироваться
- В другом лесу аутентификация не потребуется
- В лесу аутентификация не нужна

6. Какие три процесса ведут к получению доступа к ресурсу?

- **Идентификация**
- **Аутентификация**
- **Авторизация**
- Верификация

7, Выберите все объекты, с которыми можно ассоциировать (линковать) групповые политики

- **Домен**
- **Подразделение**
- **Сайт AD**
- Группа
- Компьютер

8. Какой механизм защищает от ошибок пользователя?

- RAID 5
- **Предыдущие копии**
- Кластер надежности
- Сетевая балансировка нагрузки

9. Если центра выдачи сертификатов нет, то формируется [[Самоподписанный]] сертификат?

Самоподписанный, Неавторизованный, Корневой, Доверенный

10. EFS Sharing это …

- Шифрование файлов на папке общего доступа
- Доступ к одному файлу другого пользователя добавлением его сертификата
- Доступ к одному файлу другого пользователя добавлением его в список контроля доступа
- **Шифрование на уровне каталога файловой системы**

11. Какого механизма аутентификации НЕТ в IPSecurity?

- Active Directory (Kerberos V5)
- Сертификаты
- **Предопределенный ключ**
- Локальная

12. Если вы хотите заблокировать доступ извне к одному из Web-серверов, развернутых на вашем компьютере, какие правила вам нужно будет создать?

- Заблокировать протоколы HTTP и HTTPS по порту 80
- **Заблокировать протокол HTTP по порту, заданному в конфигурации Web-сервера**
- **Заблокировать протоколы HTTPS по порту, заданному в конфигурации Web-сервера**
- Заблокировать протокол HTTP по порту 25

13. Какая технология позволяет работать с Интернет из сети с приватной адресацией?

- VPN
- Маршрутизация
- **NAT**
- Прокси
- Коммутация каналов

14. Какая технология позволяет пользователю самому восстановить предыдущее состояние своего документа?

- Предыдущая копия
- Previous Copy
- **Shadow Copy**
- Теневое копирование

15. Выберите главную проблему резервного копирования

- Файлы, заблокированные на запись и чтение другими программами
- **Длительность этого процесса**
- Большая создаваемая нагрузка на процессор

16. Какие операции обязательно выполняет SSL?

- **Шифрование трафика на сервер**
- **Шифрование трафика с сервера**
- Аутентификация пользователя
- Обеспечение целостности пакетов

17. Развертывание Proxy не требует установки и настройки специального клиента. Верно?

- Верно
- **Неверно**

18. Выберите корректное описание VPN

- **Технология, позволяющая подключить удаленного пользователя к корпоративной сети**
- Технология, позволяющая получить доступ в Интернет с подмененного IP адреса
- Технология, позволяющая спрятаться от возможности отследить ваши манипуляции в Интернет

19. Использование протокола HTTPS гарантирует …

- Аутентификацию клиента
- Аутентификацию сервера
- **Целостность трафика**
- Обход карантина

20. Выберите типы трансляции сетевых адресов

- **Статический**
- **Динамический**
- Программный
- Клиентский

21. К какому уровню модели OSI относится технология NAT?

- Канальный
- **Сетевой**
- Транспортный
- Приложений

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
5	Списки контроля доступа	
6		Коллоквиум
10	Шифрующая файловая система	
11		Коллоквиум
14	Списки контроля доступа	
15	Аутентификация. Службы каталогов сетевых ресурсов. Active Directory Групповые политики Active Directory Криптография с открытым и закрытым ключами. Сертификатфы. PKI Шифрующая файловая система Обеспечения высокого уровня доступности информации при хранении Защита информации при обработке Защита при передаче информации. Маршрутизация. SSL. IPSecurity Удаленный доступ к ресурсам сети. VPN Контроль за доступом к корпоративной сети. NIDS, NAP Контроль за доступом к внешней среде. Межсетевые экраны. Технологии NAT, пакетной и контентной фильтрации, Proxy. Публикация информации. Демилитаризованная зона.	Тест

6.4 Методика текущего контроля

На **лекционных занятиях** текущий контроль включает в себя контроль посещаемости (не менее 60 % занятий), по результатам которого студент получает допуск на экзамен.

На **лабораторных занятиях**

Порядок выполнения лабораторных работ, подготовки отчетов и их защиты:

В процессе обучения по дисциплине «Защита компьютерной информации» студент обязан выполнить минимум 6 лабораторных работ. Под выполнением лабораторных работ подразумевается подготовка к работе, проведение исследований, подготовка отчета и его защита на коллоквиуме. После каждых 4-х лабораторных работ предусматривается проведение коллоквиума на 6-й и

11-ой неделях, на которых осуществляется защита лабораторных работ. Выполнение лабораторных работ студентами осуществляется индивидуально или в бригадах до 2-х человек. Оформление отчета студентами осуществляется индивидуально в соответствии с принятыми в СПбГЭТУ правилами оформления студенческих работ. Отчет оформляется после выполнения экспериментальных исследований и представляется преподавателю на проверку путем его публикации в задании Moodl. После проверки отчет либо возвращается (при наличии замечаний) на доработку, либо подписывается к защите.

Лабораторные работы защищаются студентами индивидуально. Каждый студент получает вопрос по теоретической части, или по процедуре проведения экспериментальных исследований, или по последующей обработке результатов, после чего ему предоставляется время для подготовки ответа. При обсуждении ответа преподаватель может задать несколько уточняющих вопросов. В случае если студент демонстрирует достаточное знание вопроса, работа считается защищенной.

На защите лабораторной работы студент должен показать: понимание методики исследования и знание особенностей её применения, понимание и умение объяснять особенности применяемых методов, возможные области их применения и т.д., умение давать качественную и количественную оценку полученных результатов и прогнозировать реакции исследуемого объекта на различные воздействия, навыки и умения, приобретенные при выполнении лабораторной работы.

Текущий контроль включает в себя выполнение, сдачу в срок отчетов и их защиту по всем лабораторным работам, по результатам которой студент получает допуск на экзамен.

На практических занятиях текущий контроль включает в себя контроль посещаемости (не менее 60 % занятий), по результатам которого студент получает допуск на экзамен.

В ходе проведения **практических занятий** целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях.

Контроль **самостоятельной работы** студентов осуществляется на лекционных, лабораторных и практических занятиях студентов по методикам, описанным выше.

Итоговый тест выполняется индивидуально в среде учебного курса Moodle в отведенное для этого время.

Результаты итогового теста определяются по количеству баллов, набранных студентом в ходе выполнения теста. Результаты итогового теста используются для допуска к экзамену: допуск предоставляется при получении более 50% правильных ответов.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, проектор, экран, компьютер преподавателя	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3) Oracle VirtualBox
Лабораторные работы	Лаборатория	Количество посадочных мест с компьютерами – в соответствии с контингентом, рабочее место преподавателя	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3) Oracle VirtualBox
Практические занятия	Аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, проектор, экран, компьютер преподавателя	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3) Oracle VirtualBox
Самостоятельная работа	Помещение для самостоятельной работа	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3) Oracle VirtualBox 4) Доступ в Интернет

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА