ВычислМат_09.03.03_
УБПиП.doc

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный экономический университет»

УТВЕРЖДАЮ
Проректор по учебной и методической работе
_____/ Шубаева В.Г./
«_20_» _июня_ 20_18_ г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Рабочая программа дисциплины

Направление подготовки	09.03.03 Прикладная информатика
Направленность (профиль) программы	Управление бизнес-процессами и проектами
Уровень высшего образования	бакалавриат
Форма обучения	очная

Составители:
_____/ к.ф.-м.н., профессор Кияев В.И.

_____/ к.э.н., доцент Саитов А.В.

Санкт-Петербург
2018

СОДЕРЖАНИЕ

АННОТАЦИЯ ДИСЦИПЛИНЫ 3
1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ 5
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 5
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ 5
4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ 6
5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ 7
6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА 11
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ 13
7.1 Методические указания для обучающегося по освоению дисциплины . 13
7.2 Организация самостоятельной работы 13
8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 14
9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 14
9.1. Учебно-методическое и информационное обеспечение дисциплины 14
9.2. Материально-техническое обеспечение учебного процесса 15
10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ 16
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 17

АННОТАЦИЯ ДИСЦИПЛИНЫ

Наименование дисциплины	**Информационная безопасность**
Цель дисциплины	Заложить методически правильные основы знаний по информационной безопасности, необходимых специалистам, которые занимаются вопросами: проектирования, внедрения и эксплуатации корпоративных вычислительных и информационных систем (ВС/ИС); организацией защиты как самих систем, так и информации и данных, с которыми работают пользователи ВС/ИС.
Планируемые результаты обучения	ПК-1: Способностью проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе
Тематическая направленность дисциплины	Тема 1. Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности Тема 2. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности Тема 3. Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности Тема 4. Базовые элементы информационного правоотношения Тема 5. Виды защищаемой информации. Модель угроз и модель информационной безопасности Тема 6. Понятие защищенной информационной системы. Программа информационной безопасности Тема 7. Организационно-распорядительные документы в сфере информационной безопасности. Общая и частные политики информационной безопасности. Корпоративные стандарты ИБ Тема 8. Управление информационными рисками Тема 9. Стандартизация в сфере информационной безопасности Тема 10 Математические модели систем и процессов защиты информации Тема 11. Сервисы ИБ и защита от инсайдеров Тема 12. Криптографические методы защиты информации Тема 13. Защита информационной инфраструктуры от атак/ Антивирусные средства защиты Тема 14. Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ Тема 15. Идентификация пользователя в информационно-вычислительной системе Тема 16. Идентификация пользователя в сети Тема 17. Программное приложение KeyLemon Тема 18. Системы шифрования дисковых данных. Технология BitLocker Тема 19. Системы шифрования дисковых данных. Технология BitLocker To Go

	Тема 20. Шифрование файлов Тема 21. Шифрование дисковых данных под Linux Тема 22. Пакет McAfee Endpoint Encryption Тема 23. Пакет Symantec Drive Encryption Тема 24. Пакет Jetico BestCrypt Тема 25. Пакет TrueCrypt Тема 26. Система Symantec Desktop Email Encryption Тема 27. Система PGP NetShare
Кафедра	**Информатики**

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель дисциплины: заложить методически правильные основы знаний по информационной безопасности, необходимых специалистам, которые занимаются вопросами: проектирования, внедрения и эксплуатации корпоративных вычислительных и информационных систем (ВС/ИС); организацией защиты как самих систем, так и информации и данных, с которыми работают пользователи ВС/ИС.

Задачи:

- дать общее представление о методах, технологиях и инструментах управления информационной безопасностью, применяемых в менеджменте современной компании, а также о тенденциях совершенствования инструментария в области проектирования и управления комплексной информационной безопасности;
- дать представление о законодательном, системном и методическом обеспечении разработки систем информационной безопасности;
- ознакомить студентов с проблемами менеджмента ИБ: классификацией угроз и рисков ИБ, методами выявления угроз, отработки рисков; научить ставить и решать прикладные задачи по обеспечению информационной безопасности, надежности и эффективности ИС
- заложить методические основы знаний по разработке и стандартизации системы управления информационной безопасностью организации, по использованию стандартов информационной безопасности и методики управления процессом информационной безопасности;
- дать представление о современных, стандартах, технологиях и инструментах реализации информационной безопасности (ИБ) и защиты информации (ЗИ).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.09 «Информационная безопасность» относится к вариативной части Блока 1 и является обязательной для освоения обучающимся после выбора обучающимся направленности (профиля) программы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы представлены в таблице 3.1.

Таблица 3.1 – Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование компетенции выпускника	Этапы формирования компетенций	Планируемые результаты обучения/индикаторы достижения компетенций (показатели освоения компетенции)
ПК-1: Способностью проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к	ПК-1	Декомпозиция IV Знать: основные методологические аспекты необходимости обследования организаций, выявления информационные потребности пользователей, формирования требований к информационной системе З (IV) (ПК-1) Уметь: проводить всестороннее обследование организаций с целью оценки её текущего состояния в области информационных

информационной системе		процессов и систем, выявлять информационные потребности пользователей, формировать требования к информационной системе У (IV) (ПК-1) Владеть: сводами знаний в ИТ-сфере, стандартами, нотациями и инструментальными средствами обследования, описания и моделирования состояния организации в области зрения информационных процессов и систем, выявлять информационные потребности пользователей, формировать требования к информационной системе В(IV)(ПК-1)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов, из которых 36 часов самостоятельной работы обучающегося отводится на подготовку и защиту экзамена.

Форма промежуточной аттестации: 6-й семестр — зачет, 7-й семестр — экзамен

Распределение фонда времени по темам дисциплины по очной форме обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение фонда времени по темам дисциплины

Номер и наименование тем	Объем дисциплины (ак. часы)			
	Контактная работа			СРО
	ЗЛТ	ПЗ	ЛР	
1	2	3	4	5
6-й учебный семестр				
Тема 1. Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности	2	3		2
Тема 2. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности	2	3		2
Тема 3. Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности	2	3		2
Тема 4. Базовые элементы информационного правоотношения	2	3		2
Тема 5. Виды защищаемой информации. Модель угроз и модель информационной безопасности	1	3		2
Тема 6. Понятие защищенной информационной системы. Программа информационной безопасности	1	3		2
Тема 7. Организационно-распорядительные документы в сфере информационной безопасности. Общая и частные политики информационной безопасности. Корпоративные стандарты ИБ	1	3		2
Тема 8. Управление информационными рисками	1,5	3		2
Тема 9. Стандартизация в сфере информационной безопасности	1,5	3		2
Тема 10 Математические модели систем и процессов защиты информации	2	3		2
Тема 11. Сервисы ИБ и защита от инсайдеров	2	3		2
Тема 12. Криптографические методы защиты информации	2	3		2
Тема 13. Защита информационной инфраструктуры от атак/ Антивирусные средства защиты	2	3		2
Тема 14. Комплексная защита информационной инфраструктуры	2	3	6	10

и ресурсов. Оценка эффективности СЗИ				
Всего за 6-й семестр: 108	**24**	**42**	**6**	**36**
7-й учебный семестр				
Тема 15. Идентификация пользователя в информационно-вычислительной системе	2	1		6
Тема 16. Идентификация пользователя в сети	2	1		6
Тема 17. Программное приложение KeyLemon	2	1		6
Тема 18. Системы шифрования дисковых данных. Технология BitLocker	1,25	1,25		6
Тема 19. Системы шифрования дисковых данных. Технология BitLocker To Go	1,25	1,25		6
Тема 20. Шифрование файлов	1,25	1,25		6
Тема 21. Шифрование дисковых данных под Linux	1,25	1,25		6
Тема 22. Пакет McAfee Endpoint Encryption	1,25	1,25		6
Тема 23. Пакет Symantec Drive Encryption	1,25	1,25		6
Тема 24. Пакет Jetico BestCrypt	1,25	1,25		6
Тема 25. Пакет TrueCrypt	1,25	1,25		6
Тема 26. Система Symantec Desktop Email Encryption	2	1,5		3
Тема 27. Система PGP NetShare	2	1,5		3
Всего за 7-й семестр: 108	**20**	**16**		**72**
Всего по дисциплине: 216	**44**	**58**	**6**	**114**

*ЗЛТ – занятия лекционного типа, ПЗ – все виды занятий семинарского типа, кроме лабораторных работ, ЛР – лабораторные работы, СРО – самостоятельная работа обучающегося

5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

Тема 1. Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности

Предпосылки становления предметной области управления информационной безопасностью и общие ключевые вопросы комплексной информационной безопасности (ИБ). Анализ феномена расширения области информационных угроз с развитием информационных технологий. Экономическая и информационная безопасность предприятия.

Тема 2. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности

Развитие информационной составляющей бизнес-среды и вопросы её безопасности. Национальная политика и доктрина информационной безопасности. Уровни реализации ИБ и концепция ИБ Российской Федерации. Внешние и внутренние системные информационные угрозы. Общая инфраструктура глобальной ИБ и общая инфраструктура глобальной ИБ. Национальные интересы РФ в информационной сфере и угрозы их безопасности Концепция информационной безопасности Российской Федерации. Концептуальное видение проблемы информационной защищенности компании. Бизнес-модель компании и модель ИБ. Содержание и объекты Концепции информационной безопасности организации. Базовые правила реализации ИБ в современной компании.

Тема 3. Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности

Введение понятий информационного права. Информация: правовая и неправовая. Особенности информации в юридическом аспекте. Принципы и система информационного права. Российское и зарубежное законодательство в области информационной безопасности.

Тема 4. Базовые элементы информационного правоотношения

Базовые элементы информационного правоотношения и основные

правоустанавливающие документы. Гарантии реализации права на информацию. Принципы обеспечения права на доступ к информации. Государственная политика в сфере ИБ.

Тема 5. Виды защищаемой информации. Модель угроз и модель информационной безопасности

Информационное поле и информационный контур компании. Ключевые вопросы информационной безопасности современного предприятия. Содержание поля информационной безопасности. Общая классификация охраняемой информации. Закон РФ о коммерческой тайне, процедура реализации и управления процессом «Коммерческая тайна компании». Категории и виды угроз ИБ, ключевые области процесса анализа угроз. Ключевые области процесса анализа угроз, модель возможных угроз и основные классы методов защиты данных и информации. Типичное соотношение внутренних ИТ-угроз и распространенные пути утечки данных. Алгоритм анализа и оценки угроз, внутренние системные угрозы, пользователь ИТ, как источник угрозы. Инфраструктурные и внешние угрозы, реальные пути осуществления угроз. Концептуальная модель защиты от угроз и алгоритм формирования процесса управления информационной безопасностью. Содержание модели информационной безопасности, адаптивная модель на базе нейронных сетей с использованием нейро-нечеткого классификатора. Структура модели защиты информационных ресурсов и схема программно-аппаратного анализа на основе профилактического сканирования информационного поля компании. Формирование процесса оценки защищенности информационной среды.

Тема 6. Понятие защищенной информационной системы. Программа информационной безопасности

Колебание уровня информационной безопасности компании. Концептуальные требования защищенности корпоративной информационной системы. Модель анализа безопасности информационной системы при отсутствии злоумышленных угроз. Определение защищенности ИС, необходимое и достаточное условие безопасности ИС. Концепция гарантированности безопасности ИС. Методология анализа защищенности информационной системы. Модели системы защиты с частичным и полным перекрытием. Понятие и уровни ответственности в информационной сфере. Программа информационной безопасности компании. Мероприятия по выполнению программы ИБ: аспекты, процедуры и контроль выполнения.

Тема 7. Организационно-распорядительные документы в сфере информационной безопасности. Общая и частные политики информационной безопасности. Корпоративные стандарты ИБ

Значимость организационно-нормативных документов компании в управлении безопасностью в ИТ-сфере. Иерархия организационно-нормативных документов и уровень базовых документов в иерархии. Концепция информационной безопасности компании и сферы её приложения концепции. Политика ИБ как базовая основа процесса управления информационной безопасностью в компании. Системные требования к разработке общей политики ИБ, суть стратегического фактора ИБ. Уровни реализации политики безопасности. Правила разработки и реализации политики ИБ, взаимосвязь и детализация частных политик ИБ. Жизненный цикл политики ИБ, спиральная модель ЖЦ политики ИБ. Примеры неадекватной политики безопасности и следствий, к которым приводят такие политики, общее резюме по неудачным политикам ИБ. Корпоративные стандарты ИБ и организационно-распорядительные документы.

Тема 8. Управление информационными рисками

Влияние рисков на достижение стратегических целей компании. Взаимосвязь процессов управления бизнесом и управления экономической и информационной безопасностью в компании. Влияние ИТ-рисков на базовые показатели деятельности компании. Области применения риск-менеджмента в сфере ИТ. Определение понятия «ИТ-риск», неопределенность как источник риска. Классификация рисков, ИТ-риски и риски

программной инженерии. Специфика информационных рисков. Место управления рисками в системе управления ИБ. Общая схема менеджмента ИТ-рисков, базовые компоненты системы управления рисками. Системные действия и практические шаги по управлению рисками. Формирование процесса управления ИТ-рисками, содержание итерационного процесса управления, входы и выходы этапов процесса управления рисками. Процесс принятия решения по результатам анализа рисков. Соотношение «уровень ИТ-риска – уровень защиты», основные способы отработки рисков. Методики и программные продукты для оценки рисков. Оценка экономической эффективности системы управления рисками.

Тема 9. Стандартизация в сфере информационной безопасности

Определение стандарта, уровни представления стандартов. Приоритетные направления разработки стандартов в сфере информатизации, роль стандартов информационной безопасности. Содержание этапов стандартизации, объекты стандартизации в открытой информационной системе. Хронология стандартизации в сфере информационной безопасности. «Оранжевая книга», «Критерии оценки доверенных компьютерных систем», «Радужная серия», Европейские критерии безопасности ИТ». «Федеральные критерии безопасности ИТ», «Руководящие документы Гостехкомиссии РФ», критерии адекватности средств защиты, структура профиля защиты. Функциональные требования к доверенному вычислительному ядру ИС, требования к технологии разработки ИС с учетом требований ИБ. Британский стандарт BS 7799 (ISO/IEC 17799:2000). Единые критерии оценки безопасности информационных технологий, структура профиля защиты ИТ-продукта, иерархия и классы функциональных требований. Сравнение стандартов ИТ-безопасности, развитие семейства стандартов ISO 27000

Тема 10. Математические модели систем и процессов защиты информации

Место математических моделей в реализации защиты информации. Математические модели процессов и систем защиты информации (СЗИ). Общие требования к модели СЗИ, этапы построения модели СЗИ результаты практического моделирования. Декомпозиция модели СЗИ, контроль параметров состояния СЗИ (метрики моделей), пример модели процесса защиты. Адаптивная модель СЗИ на базе нейронных сетей, построение «хромосомы» степени угрозы и соответствующего уровня защищенности в нейросети с нечеткими связями. Объективные сложности построения моделей. Методы экспертных оценок.

Тема 11. Сервисы ИБ и защита от инсайдеров

Сервисы ИБ как реализация модели системы защиты информации. Архитектурная безопасность, схема распределенного документооборота с возможностью «обхода» СЗИ головного офиса предприятия. Феномен инсайдера в проблеме реализации ИБ, общие характеристики инсайдеров, статистический портрет инсайдера. Стандартный набор сервисов ИБ: идентификация / аутентификация пользователя, управление доступом, пример реализации контроля доступа. Механизмы целостности и контроля защищенности данных и сообщений, пример комплексного программного решения, включающего защиту от инсайдеров.

Тема 12. Криптографические методы защиты информации

Схема предприятия с распределенной информационной инфраструктурой. Базовые моменты для организации управления ИБ распределенного предприятия. Криптографические методы защиты информации. Шифрование данных и информации, виды практического шифрования, процедура шифрования информации. Требования к криптографическим СЗИ. Базовые разделы криптографии, схемы криптосистемы с закрытым и открытым ключами, шифрование на базе хэш-функций. Применение блочных алгоритмов шифрования. Управление криптографическими ключами. Стандарты шифрования в России. Электронная цифровая подпись, схема системы ЭЦП на базе алгоритма шифрования RSA.

Тема 13. Защита информационной инфраструктуры от атак/ Антивирусные средства

защиты

Содержание поля информационной безопасности компании, угрозы проникновения, ранжирование ИТ-угроз. Взлом защиты информационной инфраструктуры и вирусная опасность. Руткиты, ботнеты, виды атак с использованием ботнета, пример фишинг-атаки, рассылка спама, опасность блогерных страниц.

Компьютерные вирусы: классификация, формы организации вирусных атак, виды вредоносного программного обеспечения. Классические компьютерные вирусы, сетевые черви (Computer Worms), троянские программы, хакерские утилиты. Факторы уязвимости вычислительных и информационных систем для внедрения вредоносных программ. Признаки появления вируса.

Юридические средства борьбы с закладками, взломами и вирусами. Концептуальные положения корпоративной организации защиты от взломов и вирусной опасности, общие требования к антивирусной защите и правила для пользователей. Российские и зарубежные базовые антивирусные пакеты.

Тема 14. Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ

Распределенная ВС/ИС, построенная на Интернет-технологиях. Базовая особенность сетевых распределенных информационных структур, общие угрозы в распределенной среде. Рекомендуемые средства защиты информации в государственных органах, состав средств защиты. Четырехуровневая модель защиты распределенной системы. Схема фильтрации трафика между защищенной корпоративной и открытой сетями. Службы и протоколы системы безопасности, которые могут иметь уязвимости. Технологии межсетевых экранов: классификация и функциональные возможности. Пример политики безопасности при обмене между корпоративной и открытой сетями. Комплекс «маршрутизатор-файервол» при подключении к Internet.

Организация защиты с помощью технологии виртуальных частных сетей (VPN), способы реализации VPN-каналов. Технология защиты с использованием токенов, российские интеллектуальные карты. Биометрические средства контроля доступа, методы распознавания по изображению лица. Формирование интегральной системы ИБ, схема организации интегральной защиты информационной инфраструктуры и ресурсов, состав средств интегральной защиты. Оценка экономической эффективности интегральной системы ИБ. Развитие методов интегральной защиты.

Тема 15. Идентификация пользователя в информационно- вычислительной системе

Базовые моменты для организации управления ИБ распределенного предприятия. Криптографические методы защиты информации. Проверка пароля методом односторонней функции, возможность перехвата парольного контроля/разграничения доступа, полная хэш-защита парольного контроля/разграничения доступа. Слои защиты от подбора пароля. . Схема процедуры ИАА методом односторонней проверки. Схема полная хэш-защиты парольного контроля/разграничения доступа.

Тема 16. Идентификация пользователя в сети

Модели сессии работы пользователя в сети. Сетевые протоколы,ь обеспечивающие соединения и взаимодействие в сети. Физическое и виртуальное соединение в сети. Протоколы работы с файловыми серверами NFS и NCP.Использование принципа доверенных систем. Аутентификация на основе понятия «домена».

Тема 17. Программное приложение KeyLemon

Формирование дополнительного уровня защиты с помощью программного приложения KeyLemon. Принцип действия приложения на основе визуального контроля действий пользователя.

Тема 18. Системы шифрования дисковых данных. Технология BitLocker

Принципы и методы шифрования жесткого диска с использованием технологии BitLocker. Порядок действий при практическом шифровании дисков.

Тема 19. Системы шифрования дисковых данных. Технология BitLocker To Go

Принципы и методы шифрования жесткого диска с использованием технологии BitLocker To Go. Порядок действий при практическом шифровании.

Тема 20. Шифрование файлов

Порядок действий при практическом шифровании файлов.

Тема 21. Шифрование дисковых данных под Linux

Поддержка шифрованной файловой системы в Linux. Области защиты в Linux: системная, загрузочная, пользовательские данные, виртуальная память. Порядок действий при практическом шифровании файловой системы.

Тема 22. Пакет McAfee Endpoint Encryption

Возможности пакета. Централизованное управление. Интеграция и снижение общих расходов организации. McAfee Endpoint Encryption for Mac. McAfee Endpoint Encryption for Files and Folders. McAfee Endpoint Encryption for Removable Media. Защита данных широкого спектра устройств. Обеспечение высокой производительности персонала. Упрощение процесса управления безопасностью. Сокращение общих затрат организации. Объединение с существующей инфраструктурой.

Тема 23. Пакет Symantec Drive Encryption

Возможности пакета и ключевые преимущества: полнофункциональное решение для шифрования данных на разных платформах; возможность развертывания без участия пользователя; поддержка популярных операционных систем; двухфакторная аутентификация с использованием устройств чтения смарт-карт.

Тема 24. Пакет Jetico BestCrypt

Создание и поддержка зашифрованных виртуальных дисков. Шифрование данных несколькими алгоритмами шифрования, включая AES, Blowfish, Twofish, CAST. Основные возможности пакета: хранение зашифрованных данных в контейнерах; доступ к данным в контейнерах через виртуальные диски; шифрование набора файлов в один сжатый файл и создание самораспаковывающегося архива; шифрование и доступ к дискам через обычные разделы/тома; шифрование с использованием различных алгоритмов (AES, Blowfish, Twofish, CAST и другие); расширенная функциональность скрытия контейнеров; шифрование заголовков файлов контейнеров; возможность использования технологии Public Key Encryption для доступа к зашифрованным данным; возможность удаления заголовков зашифрованных контейнеров.

Тема 25. Пакет TrueCrypt

Принципы и методы шифрования жесткого диска с использованием технологии TrueCrypt. Порядок действий при практическом использовании пакета.

Тема 26. Система Symantec Desktop Email Encryption

Сквозное автоматическое шифрование электронной почты при передаче между клиентами без входа на сторонний веб-сайт. Основные возможности пакета: хранение ключей; групповое управление; шифрование данных.

Тема 27. Система PGP NetShare

Принципы безопасного доступа к документам, хранящимся на файловых серверах, путем автоматического и прозрачного шифрования файлов для группового доступа. Управление доступом к серверу средствами шифрования полного цикла, с указанием прав доступа для заданных групп или отдельных пользователей. Основные возможности пакета: перманентное шифрование файлов на сетевых серверах; поддержка PGP Encryption Platform; удобство в администрировании, унифицированная инфраструктура; интеграция в корпоративной среде; разделение ролей; поддержка всех основных типов документов.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/ Семинарские занятия / Лабораторные работы

№ темы	Тема занятия	Вид занятия/Наименование оценочного средства
1	2	3

6-й семестр		
Тема 1.	Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности	ПЗ: Решение практических задач по идентификации ключевых вопросов ИБ.
Тема 2	Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности	ПЗ: Решение практических задач разработке корпоративной концепции ИБ.
Тема 3	Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности	ПЗ: Решение практических задач по правовым аспектам ИБ.
Тема 4	Базовые элементы информационного правоотношения	ПЗ: Решение практических задач по формированию базовых элементов инф. правоотношения в организации.
Тема 5	Виды защищаемой информации, Модель угроз и модель информационной безопасности	ПЗ: Решение практических задач построению модели угроз.
Тема 6	Понятие защищенной информационной системы. Программа информационной безопасности	ПЗ: Решение практических задач по разработке корпоративной программы создания ИБ.
Тема 7	Организационно-распорядительные документы (ОРД) в сфере информационной безопасности. Общая и частные политики информационной безопасности. Корпоративные стандарты ИБ	ПЗ: Решение практических задач по формированию политик ИБ.
Тема 8	Управление информационными рисками	ПЗ: Решение практических задач по управлению информационными рисками КТ № 1: Презентация
Тема 9	Стандартизация в сфере информационной безопасности	ПЗ: Решение практических задач по использованию стандартов ИБ в деятельности организации.
Тема 10	Математические модели систем и процессов защиты информации.	ПЗ: Решение практических задач по построение мат. моделей ИБ.
Тема 11	Сервисы ИБ и защита от инсайдеров	
Тема 12	Криптографические методы защиты информации	ПЗ: Решение практических задач по разработке системы комплексной ИБ. КТ № 2: Презентация ЛР:Отчет
Тема 13	Защита информационной инфраструктуры от атак. Антивирусные средства защиты	
Тема 14	Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ	
7-й семестр		
Темы 15 – 17	Идентификация пользователя в информационно-вычислительной системе. Идентификация пользователя в сети.	ПЗ: Решение практических задач по отработке навыков использования различных систем доступа в систему и в сеть. КТ № 3: Показ результатов на компьютере
Темы 18,19	Программное приложение KeyLemon. Пакет TrueCrypt. Система Symantec Desktop Email Encryption. Система PGP NetShare	ПЗ: Решение практических задач по отработке навыков использования различных программных пакетов.
Темы 20, 21	Системы шифрования дисковых данных. Технология	ПЗ: Решение практических

	BitLocker. Системы шифрования дисковых данных. Технология BitLocker To Go. Шифрование файлов. Шифрование дисковых данных под Linux.	задач по отработке навыков использования систем шифрования. КТ № 4: Показ результатов на компьютере
Темы 22 - 27	Пакет McAfee Endpoint Encryption. Пакет Symantec Drive Encryption. Пакет Jetico BestCrypt.	ПЗ: Решение практических задач по отработке навыков использования различных программных пакетов.

*ПЗ – практические занятия, СЗ – семинарские занятия, ЛР – лабораторные работы

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

7.1 Методические указания для обучающегося по освоению дисциплины

Для формирования четкого представления об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине «Информационная безопасность» в самом начале учебного курса обучающийся должен ознакомиться с учебно-методической документацией:

– рабочей программой дисциплины «Информационная безопасность»: с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, перечнем знаний и умений, которыми в процессе освоения дисциплины должен владеть обучающийся,

– порядком проведения текущего контроля успеваемости и промежуточной аттестации;

– графиком консультаций преподавателей кафедры информатики ауд. 2038.

Систематическое выполнение учебной работы на занятиях лекционных и практических типов, а также выполнение самостоятельной работы позволит успешно освоить дисциплину.

В процессе освоения дисциплины «Информационная безопасность» обучающимся следует:

– слушать, конспектировать излагаемый преподавателем материал;

– ставить, обсуждать актуальные проблемы курса, быть активным на занятиях;

– задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений;

– выполнять задания практических занятий в компьютерных классах полностью и установленные сроки.

При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале не удалось, то обратится к лектору (по графику его консультаций) или к преподавателю на занятиях практического типа.

Обучающимся, пропустившим занятия (независимо от причин), не имеющим письменного решения задач или не подготовившимся к данному занятию, рекомендуется не позже чем в 2 - недельный срок явиться на консультацию к преподавателю и отчитаться по теме.

7.2 Организация самостоятельной работы

Под самостоятельной работой обучающихся понимается планируемая работа обучающихся, направленная на формирование указанных компетенций, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, без его непосредственного участия.

Виды самостоятельной работы по дисциплине представлены в таблице 7.2.1.

Таблица 7.2.1 – Организация самостоятельной работы обучающегося

№ темы	Вид самостоятельной работы
1	2
	6-й семестр
1 – 14	Подготовка к практическим занятиям по дисциплине
1 – 14	Выполнение заданий по темам дисциплины (работа по проекту)
1 – 8	Подготовка к контрольной точке № 1 (Презентация)
9 – 14	Подготовка к контрольной точке № 2 (Презентация)
14	Составление отчета по лабораторной работе
	7-й семестр
15 – 27	Подготовка к практическим занятиям по дисциплине
15 – 27	Выполнение заданий по темам дисциплины (работа по освоению программных пакетов)
15	Подготовка к контрольной точке № 3 (Результаты работы с программными пакетами)
16-20	Подготовка к контрольной точке № 4 (Результаты работы с программными пакетами)
1– 27	Подготовка к экзамену

Каждый вид СРО, указанный в таблице 7.2.1 обеспечен методическими материалами.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «Информационная безопасность» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

– проблемная лекция (тема № 1 - 3);
– лекция-дискуссия (тема № 6, 7).

Проблемная лекция. Характеризуется постановкой перед студентами учебных проблем-заданий, которые они должны самостоятельно решить, получив, таким образом, новые знания. В лекции сочетаются проблемные и информационные начала. Часть знаний студент получает в виде готовых знаний, а часть добывает самостоятельно под руководством преподавателя. На этих лекциях процесс познания студентов приближается к поисковой, исследовательской деятельности.

Лекция-дискуссия. Характеризуется тем, что преподаватель при изложении лекционного материала не только использует ответы слушателей на его вопросы, но и организует свободный обмен мнениями в интервалах между логическими разделами.

9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1. Учебно-методическое и информационное обеспечение дисциплины

Таблица 9.1.1 – Учебно-методическое обеспечение дисциплины

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	основная/ дополнительная литература	Книгообеспеченность	
		Кол-во. экз. в библ. СПбГЭУ	Электронные ресурсы
3.Кияев В.И. Комплексная информационная безопасность в управлении современным предприятием : учебное пособие / В.И. Кияев, А.В. Саитов. – Санкт-Петербург : Изд-во СПбГЭУ, 2016 . – 222 с. – Сведения доступны	**основная**	35	ЭБ OPAC.UNECON.RU

также по Интернету: opac.unecon.ru.			
2.Барабанова М. И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях : учебное пособие / М.И.Барабанова, В.И.Кияев .— 2-е изд., испр. и доп. — Санкт-Петербург : Изд-во СПбГЭУ, 2013 .— 262 с.— Сведения доступны также по Интернету: opac.unecon.ru	**дополнительная**	13	ЭБ OPAC.UNECON.RU
5.Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : Учебное пособие .— Москва ; Москва : Издательский Дом "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2019 .— 592 с.	**дополнительная**	–	ЭБС ZNANIUM

Таблица 9.1.2 – Перечень современных профессиональных баз данных (СПБД)

№	Наименование СПБД
1	Электронная библиотека Grebennikon.ru – www.grebennikon.ru
2	Научная электронная библиотека eLIBRARRY – www.elibrary.ru
3	Научная электронная библиотека КиберЛеника – www.cyberleninka.ru
4	База данных ПОЛПРЕД Справочники – www.polpred.com
5	База данных OECD Books, Papers & Statistics на платформе OECD iLibrary – www.oecd-ilibrary.org

Таблица 9.1.3 – Перечень информационных справочных систем (ИСС)

№	Наименование ИСС
1	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
2	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)
3	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
4	Электронная библиотечная система BOOK.ru - www.book.ru
5	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
6	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
7	Электронная библиотека СПбГЭУ– opac.unecon.ru

9.2. Материально-техническое обеспечение учебного процесса

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Таблица 9.2.1 – Перечень программного обеспечения (ПО)

№ п/п	Наименование ПО
1	Microsoft Windows Professional (КОНТРАКТ № 244/20 «26» июня 2020 г
2	Microsoft Office Professional (КОНТРАКТ № 244/20 «26» июня 2020 г)
3	7-Zip (freeware)
4	VirtualBox (freeware)

Лабораторные работы по дисциплине проводятся в лаборатории «Лабораторный комплекс».

Таблица 9.2.2 – Лаборатория «Лабораторный комплекс»

Вид учебных занятий	**Адрес, № аудитории**	**Лабораторное оборудование**
1	*2*	*3*
Лабораторные работы	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р», ауд. 2021	Лаборатория "Лабораторный комплекс". Специализированная мебель и оборудование: Учебная мебель на 64 посадочных места, рабочее место преподавателя, доска меловая 3-х секционная - 1 шт., доска маркерная на колесиках - 1 шт., часы - 1 шт., кафедра - 1 шт., стол - 1 шт., тумбочка - 1 шт., стул изо - 4 шт., вешалка стойка - 2 шт., жалюзи - 3 шт., Компьютер i5-8400/8GB/500GB_SSD/Viewsonic VA2410-mh - 23 шт., Ноутбук HP 250 G6 1WY58EA- 2 шт., Установка демонстрационных учебных фильмов - 1 шт., Компьютер в комплектации системный блок Intel pentium x2 g3250 клавиатура+мышь L (жесткий диск500gb,монитор philips 21.5') - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.

10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы по дисциплине с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья Университет обеспечивает:

– для инвалидов и лиц с ограниченными возможностями здоровья по зрению: размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий; присутствие ассистента, оказывающего обучающемуся необходимую помощь; выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

– для инвалидов и лиц с ограниченными возможностями здоровья по слуху: надлежащими звуковыми средствами воспроизведение информации;

– для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры, а также пребывание в указанных помещениях.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом и является приложением к рабочей программе дисциплины (модуля).