МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Санкт-Петербургский государственный экономический университет»

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Проректор по образовательной деятельности  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.Г. Шубаева  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_г. |

***Комплексная защита объектов информатизации***

**Рабочая программа дисциплины**

|  |  |
| --- | --- |
| Направление подготовки/ *Специальность* | *10.03.01 Информационная безопасность* |
| Направленность (профиль) программы/  *Специализация* | *Безопасность компьютерных систем (в экономике и управлении)* |
| Уровень высшего образования | *Бакалавриат* |
| Форма обучения | *очная* |
| Год набора | *2025* |

Составитель*(и)*:

|  |
| --- |
| к.т.н, Солодянников Александр Владимирович |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Часов по учебному плану | 144 | **Виды контроля в семестрах:**   |  | | --- | | Экзамен: семестр 7 | | Курсовая работа: семестр 7 | |
| в том числе: |  |
| контактная работа | 96 |
| самостоятельная работа | 12 |
| практическая подготовка | 0 |
| часов на контроль | 36 |

**Распределение часов дисциплины:**

|  |  |
| --- | --- |
| Семестр: | 7 |
| Вид занятий | Часы |
| Лекционные занятия | 54 |
| Практические занятия | 42 |
| Лабораторные работы |  |
| **Итого аудиторных часов** | **96** |
| Самостоятельная работа | 12 |
| Часы на контроль | 36 |
| **Итого академических часов** | **144** |
| **Общая трудоемкость в зачетных единицах** | **4** |

Санкт-Петербург

2025

**СОДЕРЖАНИЕ**

[**1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ** 3](#_Toc185244603)

[**2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ** 3](#_Toc185244604)

[**3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ** 3](#_Toc185244605)

[**4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ\*** 4](#_Toc185244606)

[**5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ** 8](#_Toc185244607)

[**5.1 Рекомендуемая литература** 8](#_Toc185244608)

[**5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства** 9](#_Toc185244609)

[**5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД)** 9](#_Toc185244610)

[**6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ** 10](#_Toc185244611)

[**7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ** 12](#_Toc185244612)

[**8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ** 13](#_Toc185244613)

[**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ** 14](#_Toc185244614)

[**1.1 Контрольные вопросы и задания к промежуточной аттестации** 14](#_Toc185244615)

[**1.2 Темы письменных работ** 16](#_Toc185244616)

[**1.3 Контрольные точки** 17](#_Toc185244617)

[**1.4 Другие объекты оценивания** 17](#_Toc185244618)

[**1.5 Самостоятельная работа обучающегося** 17](#_Toc185244619)

[**1.6 Шкала оценивания результата** 17](#_Toc185244620)

# **1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

|  |  |
| --- | --- |
| **Цель:** | Дать студентам необходимые знания в области создания системы защиты информации на предприятии, умения и навыки комплексного использования методов и средств защиты информации на объектах информатизации, создаваемых и эксплуатируемых в различных сферах народного хозяйства. |

# **2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Дисциплина Б1.О Комплексная защита объектов информатизации относится к обязательной части Блока 1.

# **3.** **ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ**

| **Код и наименование компетенции выпускника** | **Код и наименование индикатора достижения компетенций** | **Планируемые результаты обучения по дисциплине** |
| --- | --- | --- |
| ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | ОПК-6.03 - Демонстрирует знание методологии планирования, развертывания и поддержания комплекса регламентов и процедур, направленных на минимизацию рисков нарушения информационной безопасности | Знать: нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю  Уметь: организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.  Владеть: методологией планирования, развертывания и поддержания комплекса регламентов и процедур, направленных на минимизацию рисков нарушения информационной безопасности. |
| ОПК-10 - Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты | ОПК-10.02 - Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности и управлять процессом реализации защитных мер на объекте информатизации | Знать: комплексы мер по обеспечению информационной безопасности  Уметь: организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.  Владеть: навыками формирования политики информационной безопасности и управления процессами реализации защитных мер на объекте информатизации. |
| ОПК-12 - Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений | ОПК-12.02 - Способен комплексировать современные методы и средства защиты информации и применять навыки контроля эффективности комплексного применения средств и мер защиты информации | Знать: перечень исходных данных, необходимых для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений  Уметь: комплексировать современные методы и средства защиты информации.  Владеть: навыками контроля эффективности комплексного применения средств и мер защиты информации. |

# **4.** **СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ\***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Номер и наименование тем и/или разделов/тем** | **Содержание дисциплины** | | **Объем дисциплины**  **(академические часы)** | | | | |
| **Контактная работа** | | | | **СРО** |
| **ЗЛТ** | | **ПЗ** | **ЛР** |
| **Раздел I. Принципы, задачи и сущность комплексной системы защиты объектов информатизации.** | | | | | | | |
| Тема 1. Сущность и задачи комплексной защиты информации на предприятии. | Понятийный аппарат в области обеспечения информационной безопасности на предприятии. Цели, задачи и принципы построения комплексной системы защиты информации. О понятиях безопасности и защищенности. Разумная достаточность и экономическая эффективность. Управление безопасностью предприятия. Международные стандарты. Цели и задачи защиты информации в автоматизированных системах. Современное понимание методологии защиты информации: особенности национального технического регулирования, современная трактовка понятия безопасности информационных технологий, современные требования к средствам обеспечения безопасности. | | 2 | |  |  |  |
| Тема 2. Принципы организации и этапы разработки комплексной системы защиты информации. | Принципы организации и этапы разработки комплексной системы защиты информации (КСЗИ); факторы, влияющие на организацию КСЗИ. Методологические основы организации комплексной системы защиты информации. Разработка политики безопасности и регламента безопасности предприятия. Основные положения теории сложных систем. Система управления информационной безопасностью предприятия. Принципы построения и взаимодействие с другими подразделениями. Требования, предъявляемые к комплексной системе защиты информации: требования к организационной и технической составляющим комплексной системы защиты информации; требования по безопасности, предъявляемые к изделиям информационной технологии. Этапы разработки комплексной системы защиты информации. | | 4 | | 2 |  |  |
| Тема 3. Факторы, влияющие на организацию комплексной системы защиты информации. | Влияние формы собственности на особенности защиты информации ограниченного доступа. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа. Характер основной деятельности предприятия. Состав, объекты и степень конфиденциальности защищаемой информации. Структура и территориальное расположение предприятия. Режим функционирования предприятия. Конструктивные особенности предприятия. Количественные и качественные показатели ресурсообеспечения. Степень автоматизации основных процедур обработки защищаемой информации. | | 4 | | 4 |  |  |
| Тема 4. Определение и нормативное закрепление состава защищаемой информации. | Классификация информации по видам тайны и степеням конфиденциальности. Нормативно-правовые аспекты определения состава защищаемой информации. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия. Методика определения состава защищаемой информации. Порядок внедрения Перечня сведений, составляющих коммерческую тайну, внесение в него изменений и дополнений. | | 2 | | 2 |  |  |
| Тема 5. Определение объектов защиты. | Значение носителей защищаемой информации как объектов защиты. Методика выявления состава носителей защищаемой информации. Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации. Транспортные средства и особенности транспортировки. Состав средств обеспечения, подлежащих защите. | | 4 | | 4 |  | 2 |
| **Раздел II. Компоненты комплексной системы защиты объектов информатизации.** | | | | | | | |
| Тема 6. Определение компонентов комплексной системы защиты информации. | Особенности системы защиты информации (СЗИ) от несанкционированного доступа (НСД). Методика синтеза СЗИ: общее описание архитектуры АС, системы защиты информации и политики безопасности; формализация описания архитектуры исследуемой автоматизируемой системы (АС); формулирование требований к системе защиты информации; выбор механизмов и средств защиты информации; определение важности параметров средств защиты информации; оптимальное построение системы защиты для АС. Выбор структуры СЗИ АС. Проектирование системы защиты информации для существующей АС. | | 4 | | 2 |  | 2 |
| Тема 7. Предпроектное обследование объекта информатизации (на примере ИСПДн). | Содержание концепции построения комплексной системы защиты информации. Объекты защиты. Цели и задачи обеспечения безопасности информации. Основные угрозы безопасности информации АС организации. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию. Определение потенциальных каналов и методов несанкционированного доступа к информации. Определение возможностей несанкционированного доступа к защищаемой информации. Основные положения технической политики в области обеспечения безопасности информации АС организации. Основные принципы построения комплексной системы защиты информации. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Первоочередные мероприятия по обеспечению безопасности информации АС организации. | | 4 | | 4 |  | 2 |
| Тема 8. Разработка модели комплексной системы защиты информации. | Общая характеристика задач моделирования комплексной системы защиты информации. Формальные модели безопасности и их анализ: классификация формальных моделей безопасности; модели обеспечения конфиденциальности; модели обеспечения целостности; субъектно-ориентированная модель. Прикладные модели защиты информации в АС. Формальное построение модели защиты: описание объекта защиты; декомпозиция АС на субъекты и объекты; модель безопасности: неформальное описание; декомпозиция системы защиты информации; противостояние угрозам; реализация системы защиты информации субъекта АС субъектно-объектной модели. Формализация модели безопасности: процедура создания пары субъект-объект, наделение их атрибутами безопасности; осуществление доступа субъекта к объекту; взаимодействие с внешними сетями; удаление субъекта-объекта. | | 4 | | 4 |  | 2 |
| Тема 9. Кадровое обеспечение функционирования комплексной системы защиты информации. | Специфика персонала предприятия как объекта защиты. Распределение функций по защите информации: функции руководства предприятия; функции службы защиты информации; функции специальных комиссий; обязанности пользователей защищаемой информации. Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа. Подбор и обучение персонала. | | 2 | | 2 |  | 2 |
| Тема 10. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации. | Состав и значение материально-технического обеспечения функционирования комплексной системы защиты информации. Перечень вопросов защиты информации (ЗИ), требующих документационного закрепления. | | 4 | | 2 |  | 2 |
| Тема 11. Назначение, структура и содержание управления комплексной системы защиты информации. | Понятие, сущность и цели управления комплексной системой защиты информации. Принципы управления комплексной системы защиты информации. Структура процессов управления. Основные процессы, функции и задачи управления комплексной системой защиты информации. Основные стили управления. Структура и содержание общей технологии управления комплексной системой защиты информации. | | 2 | | 2 |  |  |
| Тема 12. Принципы и методы планирования функционирования комплексной системы защиты информации. | Понятие и задачи планирования функционирования комплексной системы защиты информации. Способы и стадии планирования. Факторы, влияющие на выбор способов планирования. Основы подготовки и принятия решений при планировании. Методы сбора, обработки и изучения информации, необходимой для планирования. Организация выполнения планов. | | 4 | | 2 |  |  |
| Тема 13. Сущность и содержание контроля функционирования комплексной системы защиты информации. | Виды контроля функционирования комплексной системы защиты информации. Цель проведения контрольных мероприятий в комплексной системе защиты информации. Анализ и использование результатов проведения контрольных мероприятий. | | 4 | | 2 |  |  |
| Тема 14. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций. | Понятие и основные виды чрезвычайных ситуаций (ЧС). Технология принятия решений в условиях ЧС. Факторы, влияющие на принятие решений в условиях ЧС. Подготовка мероприятий на случай возникновения ЧС. | | 4 | | 2 |  |  |
| Тема 15. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации. | Понятие и основные виды чрезвычайных ситуаций (ЧС). Технология принятия решений в условиях ЧС. Факторы, влияющие на принятие решений в условиях ЧС. Подготовка мероприятий на случай возникновения ЧС. | | 2 | | 4 |  |  |
| Тема 16. Состав методов и моделей оценки эффективности комплексной системы защиты информации. | Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса. Экономический подход к оценке эффективности комплексной системы защиты информации. | | 4 | | 4 |  |  |
| **Контроль:** | | | | | | | **36** |
| **Всего по дисциплине:** | | **54** | | **42** | |  | **12** |

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

# **5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

## **5.1 Рекомендуемая литература**

|  |  |
| --- | --- |
| **Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)** | **Электронные ресурсы** |
| 1. Солодянников А.В. Комплексная система защиты объектов информатизации : учебное пособие .— Санкт-Петербург : Изд-во СПбГЭУ, 2017 .— 91 с. — Сведения доступны также по Интернету: opac.unecon.ru . | [http://opac.unecon.ru/elibrary ... B0%D1%89%D0%B8%D1%82%D1%8B.pdf](http://opac.unecon.ru/elibrary/2015/ucheb/%D0%9A%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BD%D0%B0%D1%8F%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%20%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B.pdf) |
| 2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учебное пособие . — Электрон. дан. — М. : ИД «ФОРУМ» : ИНФРА-М, 2020. — 592 с. | <https://znanium.com/catalog/document?id=358722> |
| 3. Солодянников А.В. Информационно-аналитическая деятельность по обеспечению комплексной безопасности : учебное пособие — Санкт-Петербург : Изд-во СПбГЭУ, 2018 .— 94 с. – Сведения доступны также по Интернету: opac.unecon.ru . | [http://opac.unecon.ru/elibrary ... D%D0%BE%D1%81%D1%82%D1%8C.pdf](http://opac.unecon.ru/elibrary/2015/ucheb/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE-%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F%20%D0%B4%D0%B5%D1%8F%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C.pdf%20) |
| 4. Комплексная система защиты информации на предприятии : Методические указания к выполнению курсовой работы для студентов всех форм обучения направления подготовки 090900 Информационная безопасность, квалификация - бакалавр. Файл 11742.doc / Сост.: А.П.Кондратюк СПб : СПбГИЭУ, 2012 | <http://opac.unecon.ru/elibrary/bibl/Metod/2012/11742.doc> |

## **5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства**

|  |
| --- |
| - 7-Zip |
| - ОС Альт образование 10 |
| - LibreOffice Base |
| - LibreOffice Calc |
| - LibreOffice Writer |

## **5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД)**

|  |  |
| --- | --- |
| **№** | **Наименование СПБД/ ИСС** |
| 1. | Электронная библиотека Grebennikon.ru – [www.grebennikon.ru](http://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](http://www.polpred.com) |
| 5. | База данных OECD Books, Papers & Statistics на платформе OECD iLibrary  [www.oecd-ilibrary.org](http://www.oecd-ilibrary.org) |
| 6. | Справочная правовая система КонсультантПлюс (инсталлированный ресурс  СПбГЭУ или www.consultant.ru) |
| 7. | Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru) |
| 8. | Информационно-справочная система «Кодекс» (инсталлированный ресурс  СПбГЭУ или www.kodeks.ru) |
| 9. | Электронная библиотечная система BOOK.ru - www.book.ru |
| 10. | Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru |
| 11. | Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – [www.znanium.com](http://www.znanium.com) |
| 12. | Электронная библиотека СПбГЭУ– opac.unecon.ru |

# **6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ) групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Помещения оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

|  |  |
| --- | --- |
| **Наименование учебных аудиторий, перечень** | **Адрес (местоположение) учебных аудиторий** |
| Ауд. 1040 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 84 посадочных мест (Стол учебный 42шт., стульев 84шт), рабочее место преподавателя, доска меловая 2 шт. (односекционная), кафедра 1шт., стол 1шт., стул изо - 2шт., Переносной мультимедийный комплект: Ноутбук HP 250 G6 1WY58EA, Мультимедийный проектор LG PF1500G. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия. | 191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р» |
| Ауд. 0007 Компьютерный класс (для проведения практических занятий, курсового проектирования (выполнения курсовых работ) с применением вычислительной техники). Оборудован мультимедийным комплексом. Специализированная мебель и оборудование: Учебная мебель на 33 посадочных места, рабочее место преподавателя, доска меловая - 1 шт., доска маркерная на колесиках - 1 шт., вешалка стойка - 3 шт., жалюзи - 3 шт., Компьютер Intel Core i3 6100/ MSI H110M PRO-D/ ОЗУ DDR4 8GB 2400MHz/SSD SATA III 240Gb/Aerocool Qs-180 400W/Клавиатура + мышь Microsoft400 for Business/монитор Asus VS228DE - 24 шт., Мультимедийный проектор Тип 1 Optoma x 400 - 1 шт., Ноутбук HP 250 G6 1WY58EA - 2 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия. | 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 22 посадочных места (22 компьютерных стола, черных кресел 22шт.) Учебная мебель на 42 посадочных мест (парт 21 шт.,) рабочее место преподавателя (компьютерный стол 1шт.)доска, меловая 3-х секционная 1шт., доска маркерная на колесиках 1 ш., часы 1 шт., кафедра 1шт., стол 1шт., тумбочка 1шт., стул изо 4шт., вешалка стойка 2шт., жалюзи 3шт. Компьютер i5-8400/8GB/500GB\_SSD/Viewsonic VA2410-mh - 23 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. | 191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р» |
| Ауд. 2057 лаборатория Инженерно-технической защиты, лаборатория Программно-аппаратной защиты.Специализированная мебель и оборудование: Учебная мебель на 30 посадочных мест (Парта двухместная – 11 шт., стол – 8 шт., стулья- 30 шт.); 2 рабочих места преподавателя (2 стола, 2 стула); стол – 1 шт.; трибуна для выступлений – 1 шт.; шкаф для документов – 1 шт.; стенды настенные пробковые – 2 шт.; шкаф настенный со стеклянными створками – 4 шт.; доска для маркеров двухсторонняя – 1 шт.; персональный компьютер IBM PC-совместимый (i5-3470/RAM 8Gb/HDD 500Gb/Win7pro) – 7 шт.; персональный компьютер IBM PC-совместимый (i3-2100/RAM 8Gb/HDD 500Gb/Win7pro) – 8 шт.; коммутатор Cisco для организации локальной сети лаборатории с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации – 1 шт.; шкаф серверный 42U – 1 шт.; шкаф телекоммуникационный 20U – 1 шт.; проектор NEC ME-401X – 1 шт.; экран для проектора Screen Media Goldview 244\*244MW настенный – 1шт.; акустическая система марка Microlab модель Pro2– 1 шт.; коммутатор консольный Trend Net TK-803R – 1 шт.; разветвитель видеосигнала Aten VS-92A – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ОЭ-МР» – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ОЦТ-МР» – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ФОЭ-НР» – 1 комплект; комплект плакатов НПП «Учтех-Профи» – 1 шт.; генератор акустического шума ЛГШ-301 АО «Лаборатория ППШ» – 1 шт.; виброгенератор ЛГШ-403 в комплекте с вибропреобразователями ЛВП-2о, ЛВП-2Т АО «Лаборатория ППШ» – 1 шт.; фильтр сетевой однофазный ЛФС-10-1Ф АО «Лаборатория ППШ» – 1 шт.; генератор шума по цепям электропит., заземл. и ПЭМИ ЛГШ-503 АО «Лаборатория ППШ» – 1 шт.; устройство защиты телефонных линий Гранит-8 абонентское АО «Лаборатория ППШ» – 1 шт.; сервер HP-DL – 5 шт.; Коммутатор Cisco Small Business SF302-08 – 4 шт.; Коммутатор Cisco 2950 – 3 шт.; Коммутатор Cisco 3560 – 1 шт.; Беспроводной маршрутизатор TP-Link TL -WR941 ND; Электронные ключи Guardant – 16 шт.; огнетушитель ОУ-5 – 1 шт.; огнетушитель ОП-4(3)-ВСЕ – 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия. | 191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р» |

# **7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ**

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться со следующими документами:

* учебно-методической документацией;
* локальными нормативными актами, регламентирующими основные вопросы организации и осуществления образовательной деятельности, в том числе регламентирующие порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся;
* графиком консультаций сотрудников профессорско-преподавательского состава.

Уровень и глубина освоения дисциплины определяются активной и систематической работой обучающихся на лекционных занятиях, занятиях семинарского типа, выполнением самостоятельной работы, в том числе в части выделения наиболее значимых и актуальных проблем для дальнейшего изучения. Особым условием качественного освоения дисциплины является эффективная организация труда, позволяющая распределить учебную нагрузку равномерно в соответствии с графиком учебного процесса.

При подготовке к учебным занятиям обучающимся предоставляется возможность посещения консультаций сотрудников профессорско-преподавательского состава СПбГЭУ согласно расписанию, установленному в графике консультаций.

Аудиторная и внеаудиторная работа обучающихся должна быть направлена на формирование:

* фундаментальных основ мировоззрения обучающихся и естественнонаучного познания;
* базисных знаний, соответствующих направлению подготовки и заявленной профессиональной области, формирующих целевую и профессиональную основу для подготовки кадров;
* профессиональных компетенций ориентированных на удовлетворение потребностей рынка труда;
* индивидуальной траектории посредством освоения уникального набора профессиональных компетенций дополняющих компетентностную модель обучающегося, за счет ориентации на конкретные профессиональные специализированные области знаний, определяемые представителями рынка труда;
* метанавыков обучающихся, таких как: командная работа и лидерство, анализ данных, цифровые навыки, разработка и реализация проектов, межкультурное взаимодействие.

# **8. 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 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.

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья. Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

# **ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

## **1.1 Контрольные вопросы и задания к промежуточной аттестации**

|  |  |
| --- | --- |
| 1 | Цель, задачи, принципы и составные части комплексной системы защиты информации (КСЗИ) типового предприятия. |
| 2 | Системообразующие связи между составными частями КСЗИ предприятия. Основные принципы организации и этапы разработки КСЗИ предприятия. |
| 3 | Постоянные внешние и внутренние факторы, определяющие устойчивость функционирования КСЗИ при их воздействии. |
| 4 | Случайные внешние и внутренние факторы, учитываемые при построении КСЗИ, в том числе техногенные катастрофы и чрезвычайные ситуации. |
| 5 | Объективные и субъективные факторы. Факторы стоимости и эффективности, необходимости и достаточности построения КСЗИ. |
| 6 | Психологические и поведенческие факторы работников предприятия, учитываемые при разработке и построении КСЗИ. |
| 7 | Краткая законодательная база в области отнесения информации к различным категориям конфиденциальности. |
| 8 | Составление и документальное оформление перечней защищаемой конфиденциальной информации. |
| 9 | Определение мест хранения и носителей защищаемой информации. |
| 10 | Ограничение и документальное оформление круга лиц, допущенных к защищаемой информации. Определение точек доступа доверенных лиц к защищаемой информации. |
| 11 | Анализ информационных потоков защищаемой информации. Определение состава объектов защиты по видам и категориям конфиденциальности. |
| 12 | Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на защищаемую информацию. |
| 13 | Определение возможностей несанкционированного доступа к защищаемой информации. |
| 14 | Документальное оформление всех выявленных групп потенциальных источников угроз безопасности информации. |
| 15 | Ранжирование различных групп потенциальных источников угроз безопасности информации по степени опасности. |
| 16 | Построение и документальное оформление комплексной модели угроз безопасности информации на предприятии. Определение порядка и условий изменения разработанной комплексной модели угроз |
| 17 | Проверка адекватности построенной модели угроз требованиям максимальной комплексности и минимальной необходимости и ее чувствительности при изменении внутренних и внешних дестабилизирующих факторов. |
| 18 | Понятие рефлексивного управления. Определение дополнительных объектов защиты и точек доступа к информации, не представляющей ценности для предприятия. |
| 19 | Построение и документальное оформление комплексной модели угроз безопасности информации на предприятии с учетом дополнительной модели рефлексивного управления угрозами. |
| 20 | Проверка адекватности и чувствительности построенной модели угроз с учетом рефлексивного управления. |
| 21 | Разработка модели комплексной системы защиты информации на предприятии. Технологическое и организационное построение КСЗИ. |
| 22 | Сравнительная оценка моделей угроз безопасности информации и комплексной системы защиты информации. Выявление уязвимых звеньев разработанной модели защиты. |
| 23 | Корректировка комплексной системы защиты информации на предприятии. Определение порядка и условий изменения модели защиты при изменении модели угроз. |
| 24 | Составление аналитического обоснования и технического задания на проектирование комплексной системы защиты информации на предприятии. |
| 25 | Определение соотношения правовых, организационных, технических, программных, аппаратных, программно-аппаратных компонентов защиты информации, а также этических норм в комплексной модели защиты информации на предприятии. |
| 26 | Экспертная оценка соответствия предлагаемых компонентов защиты информации различным группам угроз безопасности информации в действующей модели угроз и частным угрозам в группах. |
| 27 | Порядок корректировки состава компонентов КСЗИ при изменении содержания модели угроз или их несоответствия модели. |
| 28 | Разработка технических проектов составных частей комплексной системы защиты информации и рабочей документации. |
| 29 | Определение и документальное оформление перечня правовых и организационных мер защиты информации. |
| 30 | Выбор и экспертная оценка технических, аппаратных, программных и аппаратно-программных средств защиты информации. |
| 31 | Определение поставщиков и закупка выбранных средств защиты. Порядок внесения изменений в технические проекты. |
| 32 | Порядок внедрения организационных мер защиты информации на предприятии. |
| 33 | Монтажные работы по установке и внедрению технических средств защиты информации. Установка и настройка программных, аппаратных, программно-аппаратных средств защиты информации. |
| 34 | Порядок доведения этических норм, правовых и законодательных мер по защите информации. |
| 35 | Объединение компонентов защиты в систему. Опытная эксплуатация комплексной системы защиты информации на предприятии. |
| 36 | Аттестационные испытания отдельных составных частей комплексной системы защиты информации на предприятии и аттестация системы защиты в целом. Ввод в эксплуатацию. |
| 37 | Система образования России в сфере защиты информации. Перечень необходимых специальностей по защите информации для обеспечения комплексности защиты информации на предприятии. Периодичность повышения квалификации специалистов по защите информации |
| 38 | Состав органов защиты информации предприятия. Понятие о трудоемкости обеспечения функционирования КСЗИ в процессе эксплуатации. |
| 39 | Порядок финансирования эксплуатации КСЗИ предприятия. Материально-техническое обеспечение технического обслуживания КСЗИ предприятия. |
| 40 | Порядок взаимодействия с внешними лицензированными организациями по вопросам технического обслуживания. |
| 41 | Создание подменного фонда средств защиты информации. Порядок горячей замены средств защиты информации. |
| 42 | Порядок модернизации и развития КСЗИ предприятия. |
| 43 | Законодательная база по вопросам функционирования КСЗИ предприятия. База этических норм регулирования эксплуатации КСЗИ. |
| 44 | Нормативно-методическое обеспечение эксплуатации КСЗИ на предприятии. Виды ответственности за нарушение законодательства в сфере защиты информации. |
| 45 | Руководящие документы ФСТЭК России по оценке защищенности КСЗИ. |
| 46 | Назначение, структура и содержание управления КСЗИ предприятия. Принципы и методы планирования функционирования КСЗИ. |
| 47 | Сущность и содержание контроля функционирования КСЗИ. |
| 48 | Виды управления КСЗИ предприятия. Принципы и содержание автоматизированного управления КСЗИ предприятия. Понятие об автоматизированном рабочем месте управления КСЗИ предприятия. |
| 49 | Цель и задачи рефлексивного управления КСЗИ предприятия. Использование дополнительных элементов модели угроз безопасности информации в целях рефлексивного управления |
| 50 | Организация ложных компонентов КСЗИ предприятия для дезинформации потенциальных злоумышленников. |
| 51 | Организация пункта контроля эксплуатации КСЗИ предприятия в интересах рефлексивного управления |
| 52 | Организация активных воздействий на КСЗИ предприятия в целях ее взлома. |
| 53 | Законодательная база по вопросам управления функционированием КСЗИ предприятия в условиях чрезвычайных ситуаций и техногенных катастроф. |
| 54 | Первичные мероприятия по эвакуации объектов защиты в чрезвычайной ситуации. |
| 55 | Порядок уничтожения защищаемой информации в условиях чрезвычайных ситуаций. Архивирование защищаемой информации. |
| 56 | Нормативно-методическое обеспечение передачи в другие организации и уничтожения защищаемой информации в условиях чрезвычайных ситуаций. Технические средства уничтожения защищаемой информации. |
| 57 | Цель и задачи оценки эффективности функционирования КСЗИ предприятия. Критерии эффективности. |
| 58 | Методы оценки эффективности. Экспертные модели оценки эффективности. Математические модели оценки эффективности. |
| 59 | Этапы оценки эффективности. Алгоритмы оценки эффективности на каждом этапе. |
| 60 | Использование результатов оценки эффективности функционирования КСЗИ предприятия в целях модернизации и развития. |

## **1.2 Темы письменных работ**

|  |  |
| --- | --- |
| 1 | Методика учета психологических и поведенческих факторов работников предприятия при построении и эксплуатации КСЗИ. |
| 2 | Методика определения защищаемой информации, технологической схемы ее хранения, обработки и передачи. |
| 3 | Методика определения факторов, влияющих на организацию КСЗИ в зависимости от типа объекта защиты и характера решаемых задач. |
| 4 | Обзор типовых и перспективных моделей комплексной системы защиты информации на предприятии. |
| 5 | Учет факторов, влияющих на организацию КСЗИ по критериям «стоимость/эффективность и необходимость/достаточность. |
| 6 | Методика выбора рационального состава компонентов КСЗИ на предприятии. |
| 7 | Методика аттестационных испытаний комплексной системы защиты информации на предприятии с целью выявления уязвимостей. |
| 8 | Методика определения соотношения различных групп компонентов КСЗИ на предприятии. |
| 9 | Содержание материально-технического обеспечения функционирования КСЗИ на предприятии. |
| 10 | Экспертные методики оценки эффективности функционирования КСЗИ предприятия. |
| 11 | Этапы жизненного цикла КСЗИ на предприятии. |
| 12 | Методика объединения отдельных компонентов КСЗИ в систему. |
| 13 | Оптимизация состава органов защиты информации в зависимости от решаемых задач на предприятии. |
| 14 | Управление КСЗИ объекта защиты на этапе эксплуатации. |
| 15 | Методика поддержания аттестованного объекта защиты в актуальном состоянии. |
| 16 | Рефлексивное управление КСЗИ на предприятии. |
| 17 | Управление КСЗИ предприятия в условиях чрезвычайных ситуаций и техногенных катастроф. |
| 18 | Математические методы оценки эффективности функционирования КСЗИ предприятия. |
| 19 | Построение комплексной модели угроз безопасности информации на предприятии. |
| 20 | Определение ценности защищаемой информации и стоимости затрат на ее защиту. |
| 21 | Методика определения состава компонентов КСЗИ предприятия и принципов ее построения. |
| 22 | Порядок разработки технорабочего проекта КСЗИ на предприятии. |

## **1.3 Контрольные точки**

|  |  |  |  |
| --- | --- | --- | --- |
| **Номер контрольной точки** | **Тип контрольной точки** | **Способ проведения** | **Номера тем** |
| 1 | Контрольная работа | с помощью технических средств и информационных систем | 1-6 |
| 2 | Контрольная работа | с помощью технических средств и информационных систем | 9-13 |
| 3 | Текущий контроль | с помощью технических средств и информационных систем | 14-16 |

## **1.4 Другие объекты оценивания**

|  |  |
| --- | --- |
|  | Рабочей программой дисциплины не предусмотрено. |

## **1.5 Самостоятельная работа обучающегося**

|  |  |
| --- | --- |
| **Наименования самостоятельной работы** | **Номера тем** |
| Подготовка сообщений, докладов | 1-6 |
| Курсовое проектирование | 1-16 |
| Подготовка к экзамену | 1-16 |

## **1.6** **Шкала оценивания результата**

Шкалы оценивания и процедуры оценивания результатов обучения **по дисциплине** регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования и Положением о балльно-рейтинговой системе.

Для оценки сформированности результатов обучения по дисциплине используется **балльно-рейтинговая система успеваемости обучающихся**:

Формой итогового контроля по дисциплине является экзамен (или дифференцированный зачет), итоговая оценка формируется в соответствии со шкалой, приведенной ниже в таблице:

|  |  |
| --- | --- |
| Баллы | Оценка |
| <=54 | неудовлетворительно |
| 55-69 | удовлетворительно |
| 70-84 | хорошо |
| >=85 | отлично |

**Шкала оценивания результата**

|  |  |
| --- | --- |
| 2 (балл до 54) | Демонстрирует непонимание проблемы. Многие требования, предъявляемые к заданию не выполнены.  Демонстрируется первичное восприятие материала. Работа незакончена и /или это плагиат. |
| 3 (балл 55-69) | Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены.  Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер. |
| 4 (балл 70-84) | Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены.  Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения. |
| 5 (балл 85-100) | Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены.  Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостных характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход. |