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

УТВЕРЖДАЮ
Проректор по учебной и методической работе
_____/Шубаева В.Г./
«22» августа 20 20 г.

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Рабочая программа дисциплины

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль) программы	Безопасность компьютерных систем (в экономике и управлении)
Уровень высшего образования	бакалавриат
Форма обучения	очная

Составитель:
_____/к.ф.-м.н., доцент Васильева И.Н.

Санкт-Петербург
2020

СОДЕРЖАНИЕ

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

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель (цели) освоения дисциплины: изучение принципов построения и практического применения криптографических протоколов для решения профессиональных задач в области информационной безопасности.

Задачи:

- формирование представлений об основных понятиях, роли, области применения и способов реализации криптографических протоколов в современных программных комплексах;
- приобретение теоретических знаний о принципах построения и анализа стойкости криптографических протоколов, основных протоколах аутентификации, выработки ключей, обеспечения целостности и конфиденциальности;
- формирование умения формулировать количественные и качественные требования к криптографическим протоколам при решении практических задач обеспечения информационной безопасности;
- формирование умения осуществлять выбор протоколов и настройку параметров криптографии в защищенных информационных системах;
- формирование практических навыков установки, настройки и администрирования средств криптографической защиты информации;
- формирование навыков использования криптографических методов и средств для реализации требований политики безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В «Криптографические протоколы» 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 выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Второй уровень (углубленный) (ПК-1) –2	Декомпозиция I Знать: принципы построения криптографических протоколов и способы их реализации в компьютерных системах, назначение, функции и принципы построения средств криптографической защиты информации З2 (I)(ПК-1) Уметь: применять средства криптографической защиты информации для решения профессиональных задач У2(I) (ПК-1) Владеть: навыками установки, настройки и администрирования средств криптографической защиты информации В2 (I)(ПК-1)
ПК-4 – способностью	Первый	Декомпозиция III

участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	уровень (пороговый) (ПК-4) –1	Знать: области применения и назначение криптографических протоколов, основные протоколы аутентификации, выработки ключей, обеспечения целостности и конфиденциальности З1 (III)(ПК-4) Уметь: производить выбор криптографических протоколов и настройку параметров криптографии в системах криптографической защиты информации У1(III) (ПК-4) Владеть: навыками использования криптографических методов и средств для реализации требований политики безопасности В1 (III)(ПК-4)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

Форма промежуточной аттестации: дифференцированный зачет (зачет с оценкой) – 7 семестр.

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

Таблица 4.1 – Распределение фонда времени по темам дисциплины (очная форма обучения)

Номер и наименование тем	Объем дисциплины (ак. часы)			
	Контактная работа			СРО
	ЗЛТ	ПЗ	ЛР	
1	*2*	*3*	*4*	*5*
Тема 1.1. Основы теории криптографических протоколов	2			10
Тема 1.2. Выработка криптографического ключа на основе пароля	2	2		10
Тема 1.3. Протоколы аутентификации	4	2		12
Тема 1.4. Распределение открытых ключей	2	8		12
Тема 1.5. Распределение и согласование секретных ключей	4	8		12
Тема 1.6. Защищенные сетевые протоколы	2	6		12
Тема 2.1. Специальные схемы цифровой подписи и протоколы финансовой криптографии	4	4		12
Тема 2.2. Разделение секрета	2	2		10
Всего по дисциплине:	**22**	**32**		**90**

*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

Раздел 1. Основные криптографические протоколы и методы реализации криптографической защиты

Тема 1.1. Основы теории криптографических протоколов

Криптографические примитивы и криптографические протоколы. Виды криптографических протоколов. Формальное описание протокола. Компрометация протокола. Виды атак на криптографические протоколы. Методы анализа протоколов. Основные подходы к конструированию безопасных протоколов.

Тема 1.2. Выработка криптографического ключа на основе пароля

Проблема подбора пароля. Алгоритм выработки криптографического ключа из пароля. Функции диверсификации ключа PBKDF2, scrypt. Контроль целостности PBMAC1 и шифрование PBEC2. Практические реализации парольной защиты ключевой информации.

Тема 1.3. Протоколы аутентификации

Простейшие протоколы односторонней аутентификации с предраспределенным ключом. Парольная аутентификция.

Схемы аутентификации вида «запрос - ответ». Схемы аутентификации для мобильных устройств.

Интерактивные системы доказательств с нулевым разглашением. Аутентификация с нулевым разглашением.

Методы анализа схем аутентификации.

Тема 1.4. Распределение открытых ключей

Проблема компрометации открытого ключа при передаче. Цифровые сертификаты. Модели доверия на основе цепей сертификации. Инфраструктура открытых ключей PKI.

Тема 1.5. Распределение и согласование секретных ключей

Свойства протоколов распределения ключей.

Предварительное распределение ключей. Схема Блома.

Протокол выработки общего ключа с аутентификацией на основе пароля.

Протоколы распределения ключей с доверенным центром, основанные на симметричных криптосистемах. Протокол Kerberos. Расширение протокола Kerberos PKINIT для использования криптографии с открытым ключом.

Протокол Диффи-Хэллмана формирования общего секретного ключа и его обобщения. Протоколы MTI и STS.

Схемы выработки общего ключа с аутентификацией на основе открытого ключа. Протокол Нидхема-Шредера.

Протоколы обновления сеансовых ключей.

Методы анализа протоколов распределения ключей.

Тема 1.6. Защищенные сетевые протоколы

Понятие безопасности протокола. Функции-сервисы безопасности.

Протоколы каналов защищенной передачи данных PPTP, L2TP, IPSec, SSL/TLS, SHH. Алгоритмы, используемые защищенными сетевыми протоколами: согласование ключей VKO, алгоритм диверсификации KDF, псевдослучайные функции на основе конструкции HMAC (в протоколах TLS, IPSec), экспорт и импорт ключей.

Шифрование в мессенджерах.

Раздел 2. Специальные применения криптографических протоколов

Тема 2.1. Специальные схемы цифровой подписи и протоколы финансовой криптографии

Цифровая подпись с восстановлением сообщения. Протокол подписи с ограниченным жизненным циклом. Схема подписи с верификацией по запросу (Казаринов). Групповая цифровая подпись. Пороговая цифровая подпись. Слепая цифровая подпись и ее применения.

Системы электронных платежей и электронные деньги. Электронные банкноты Шаума. Децентрализованные системы электронных платежей. Криптовалюты. Технология блокчейн.

Тема 2.2. Разделение секрета

Основные понятия и простейшие схемы разделения секрета. Пороговые схемы разделения секрета. Совершенность и идеальность схемы разделения секрета. Проверяемое разделение секрета.

Протокол конфиденциальных вычислений.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/Семинарские занятия/Лабораторные работы

№ темы	Тема занятия	Вид занятия/Оценочное средство
1	*2*	*3*
1.2	Задача 1. Изучение криптографических средств ОС Linux	ПЗ, Решение практических задач, отчет
1.3	Задача 2. Изучение схем аутентификации с нулевым разглашением	ПЗ, Решение практических задач, отчет
1.4	Задача 3. Развертывание PKI инфраструктуры в корпоративной сети	ПЗ, Решение практических задач, отчет
	Задача 4. RSA-сертификаты. Статическая аутентификация данных	
	Задача 5. RSA-сертификаты. Динамическая аутентификация данных	
	Задача 6. RSA-сертификаты. Комбинированная динамическая аутентификация данных и выработка криптограммы	
1.5	Задача 7. Настройка Kerberos аутентификации в корпоративной сети	ПЗ, Решение практических задач, отчет
1.6	Задача 8. Работа с пакетом криптографических функций OpenSSL в режиме командной строки	ПЗ, Решение практических задач, отчет
2.1	Задача 9. Изучение системы электронных денег Чаума	ПЗ, Решение практических задач, отчет. Исследование (эссе)
	Задача 10. Изучение технологии блокчейн	
2.2	Задача 11. Изучение пороговой схемы Шамира разделения секрета	ПЗ, Решение практических задач, отчет

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 в самом начале учебного курса обучающийся должен ознакомиться с учебно-методической документацией:

- рабочей программой дисциплины: 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.

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

В процессе освоения дисциплины 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 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 семинарского 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.

Методическое обеспечение самостоятельной работы при наличии обучающихся лиц с ограниченными возможностями представляется в формах, адаптированных к ограничениям их здоровья.

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*
1.1	Изучение литературных источников, подготовка по контрольным вопросам.
1.2	Изучение нормативных и литературных источников, подготовка к ПЗ, подготовка по контрольным вопросам.
1.3	Изучение литературных источников, подготовка к ПЗ, подготовка к контрольной точке №2, подготовка по контрольным вопросам.
1.4	Изучение литературных источников, подготовка к ПЗ, подготовка к контрольной точке №2, подготовка по контрольным вопросам.
1.5	Изучение нормативных и литературных источников, подготовка к ПЗ, подготовка к контрольной точке №2, подготовка по контрольным вопросам.
1.6	Изучение нормативных и литературных источников, подготовка к ПЗ, подготовка к контрольной точке №2, подготовка по контрольным вопросам.
2.1	Изучение литературных источников, подготовка к ПЗ, подготовка по контрольным вопросам.
2.2	Изучение литературных источников, подготовка к ПЗ, подготовка по контрольным вопросам.
1.1	Подготовка к контрольной точке №1.
2.1	Подготовка к контрольной точке №2.

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

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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

Активные и интерактивные методы обучения:

К интерактивным методам обучения относится выполнение индивидуальных заданий на ПК в ходе практических занятий и самостоятельной работы по темам 1.2, 1.3, 1.4, 1.5, 1.6, 2.1, 2.2.

Выполнение индивидуальных заданий на ПК предполагает решение практических задач по моделированию и реализации действий сторон в криптографических протоколах с помощью пакетов прикладных программ; установке, настройке и администрированию программных средств криптографической защиты информации; изучению информационно-коммуникационных технологий, базирующихся на использовании криптографических протоколов.

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**
Ищукова Е.А. Криптографические протоколы и стандарты : учебное пособие / Ищукова Е.А., Лобова Е.А. — Электрон. дан. - Таганрог:Южный федеральный университет, 2016. - 80 с.	основная	–	ЭБС ZNANIUM
Запечников С.В. Криптографические методы защиты информации : учебник / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Электрон. дан. — Москва : Издательство Юрайт, 2018. — 309 с.	основная	–	ЭБС Юрайт
Фомичёв В.М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Электрон. дан. — Москва : Издательство Юрайт, 2018. — 245 с.	дополнительная	–	ЭБС Юрайт
Васильева И.Н. Криптографические методы защиты информации : учебник и практикум / И. Н. Васильева. — Электрон. дан. — Москва : Издательство Юрайт, 2017. — 349 с.	дополнительная	–	ЭБС Юрайт

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	Oracle Virtual Box (freeware)
5	ОС Kali Linux (freeware)

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 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).