**Санкт-Петербургский государственный университет**

**Р А Б О Ч А Я П Р О Г Р А М М А**

**УЧЕБНОЙ ДИСЦИПЛИНЫ**

Современные подходы к хранению, управлению и защите данных

Modern Approaches to Data Storage, Management and Protection

**Язык(и) обучения**

русский

Трудоемкость в зачетных единицах: 3

Регистрационный номер рабочей программы: 030373

Санкт-Петербург

2020

**Раздел 1. Характеристики учебных занятий**

**1.1. Цели и задачи учебных занятий**

Целью курса является знакомство обучающихся с основными методами криптографии, применяемыми в защите информации. В результате изучения курса обучающиеся должны получить представление об основном криптографическом инструментарии, необходимом для использования защищенных информационных систем.

Содержание дисциплины охватывает круг вопросов, связанных с защитой компьютерной информации, способами хранения и передачи информации, в курсе осуществляется знакомство с существующими методами защиты информации и применяемыми информационными технологиями для хранения и передачи информации.

**1.2. Требования подготовленности обучающегося к освоению содержания учебных занятий (пререквизиты)**

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

* информатика;
* дискретная математика;
* теория вероятностей и мат. статистика.

Желательным является изучение курса «Основы компьютерной безопасности» или аналогичного.

**1.3. Перечень результатов обучения (learning outcomes)**

В процессе изучения дисциплины «Современные подходы к хранению, управлению и защите данных» обучаемые приобретают следующие знания:

* понятия компьютерной безопасности – доступность, целостность, конфиденциальность;
* историю и современные тенденции построения безопасных систем;
* подходы и методы поиска уязвимостей и способы их устранения;
* соблюдать основные требования информационной безопасности;
* реализовывать решения, направленные на защиту сетевых сервисов и обнаружения вероятной атаки;
* изучат основные методы передачи информации, симметричное и ассиметричное шифрование;
* использовать в научной и познавательной деятельности, а также в социальной сфере профессиональные навыки работы с информационными и компьютерными технологиями;
* критически переосмысливать свой опыт, адаптироваться к различным ситуациям, проявлять творческий подход, инициативу и настойчивость в достижении целей профессиональной деятельности;
* делать анализ и грамотную оценку эффективности разрабатываемых методов защиты информации;
* работы с информацией из различных источников, включая сетевые ресурсы сети Интернет, для решения профессиональных задач;
* осуществления целенаправленного поиска информации о технологических достижениях в сети Интернет и из других источников;
* применения в профессиональной деятельности современных средств защиты компьютерных систем;

Иметь базовые представления о системах безопасности, методах хранения и передачи информации, методах взлома, вероятных векторов атак, организация сложной многоуровневой защиты.

Уметь формализовывать поставленные задачи и реализовывать сложные программные комплексы защиты с точки зрения грамотной профессиональной разработки различного рода проектов.

Дисциплина способствует развитию следующих компетенций:

* ПКА-1 – способен находить, формулировать и решать актуальные проблемы фундаментальной и прикладной информатики и информационных технологий;
* ПКП-1 – способен демонстрировать фундаментальные знания математических и естественных наук, программирования и информационных технологий;
* ПКП-8 – способен использовать основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования, методы, способы и средства разработки программ в рамках этих направлений.

**1.4. Перечень и объём активных и интерактивных форм учебных занятий**

Аудиторная учебная работа (10 часов): интерактивныелекции; практические занятия.

**Раздел 2. Организация, структура и содержание учебных занятий**

**2.1. Организация учебных занятий**

**2.1.1 Основной курс**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Трудоёмкость, объёмы учебной работы и наполняемость групп обучающихся | | | | | | | | | | | | | | | | | | |
| Код модуля в составе дисциплины,  практики и т.п. | Контактная работа обучающихся с преподавателем | | | | | | | | | | | | Самостоятельная работа | | | | Объём активных и интерактивных  форм учебных занятий | Трудоёмкость |
| лекции | семинары | консультации | практические  занятия | лабораторные работы | контрольные работы | коллоквиумы | текущий контроль | промежуточная  аттестация | итоговая аттестация | под руководством преподавателя | в присутствии  преподавателя | сам. раб. с использованием  методических материалов | текущий контроль (сам.раб.) | промежуточная аттестация (сам.раб.) | итоговая аттестация  (сам.раб.) |
| ОСНОВНАЯ ТРАЕКТОРИЯ | | | | | | | | | | | | | | | | | | |
| Форма обучения: очная | | | | | | | | | | | | | | | | | | |
| Семестр 2 | 30 |  | 2 | 15 |  |  |  |  | 2 |  |  |  | 65 |  | 30 |  | 10 | 4 |
|  | 2-100 |  | 2-100 | 2-30 |  |  |  |  | 1-100 |  |  |  | 1-1 |  | 1-1 |  |  |  |
| ИТОГО | 30 |  | 2 | 15 |  |  |  |  | 2 |  |  |  | 65 |  | 30 |  |  | 4 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Виды, формы и сроки текущего контроля успеваемости и промежуточной аттестации | | | | | | |
| Код модуля в составе дисциплины, практики и т.п. | Формы текущего контроля успеваемости | | Виды промежуточной аттестации | | Виды итоговой аттестации  (только для программ итоговой аттестации и дополнительных образовательных программ) | |
| Формы | Сроки | Виды | Сроки | Виды | Сроки |
| ОСНОВНАЯ ТРАЕКТОРИЯ | | | | | | |
| Форма обучения: очная | | | | | | |
| Семестр 2 |  |  | экзамен, устно, традиционная форма | по графику промежуточной аттестации |  |  |

**2.2. Структура и содержание учебных занятий**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п.п.** | **Наименование темы (раздела, части)** | **Вид учебных занятий** | **Кол-во часов** |
| 1 | Раздел 1. Введение.  Раздел 2. Основы классической криптографии  Раздел 3. Вопросы криптографической стойкости шифров, основные понятия, модели  и методы криптоанализа симметричных систем.  Раздел 4. Современные блочные шифры с секретным ключом. | лекции | 16 |
| практические занятия | 7 |
| по методическим материалам | 32 |
| 2 | Раздел 5. Принципы построения и реализации криптографических алгоритмов поточных шифров.  Раздел 6. Асимметричные криптосистемы.  Раздел 7. Криптографические функции хэширования и контроль целостности информации.  Раздел 8. Криптографические протоколы | лекции | 14 |
| практические занятия | 8 |
| по методическим материалам | 33 |
| 3 | Промежуточная аттестация | самостоятельная работа | 30 |
| консультации | 2 |
| экзамен | 2 |
| **Итого** | | | **144** |

*Раздел 1. «Введение».*

Краткая историческая справка развития криптографии. Криптография и стеганография.

Основные термины и понятия. Открытый текст и его основные свойства. Энтропия открытого текста. Математические модели открытых текстов.

*Раздел 2. «Основы классической криптографии».*

Классификация методов шифрования: симметричное и ассиметричное шифрование.

Понятие о ключе и шифре. Математические модели шифров. Простейшие шифры и их свойства. Шифры перестановки и замены (моноалфавитный и полиалфавитная подстановка). Комбинированные шифры. Классические поточные шифры: гаммирования и замены.

*Раздел 3. «Вопросы криптографической стойкости шифров, основные понятия, модели и методы криптоанализа симметричных систем».*

Теоретическая и практическая стойкость шифров. Условная и безусловная стойкость.

Абсолютно стойкий шифр. Энтропия шифртекста и ключа. Расстояние единственности для открытого текста и ключа. Совершенные шифры: их достоинства и недостатки. Длина секретного ключа и стойкость криптоалгоритма. Основные требования к шифрам. Влияние секретности алгоритма шифрования и длины ключа на стойкость криптоалгоритма. Принцип Керкхоффа. Проблема оценки стойкости условно стойких шифров. Количественные оценки числа операций и используемой памяти при проведении криптоаналитической атаки. Криптографические и некриптографические методы вскрытия шифров. Основные типы криптографических нападений (атак): на основе шифротекста, на основе известного текста, на основе специально подобранных текстов, на основе адаптированных текстов.

*Раздел 4. «Современные блочные шифры с секретным ключом».*

Блочный шифр - шифр простой замены. Криптоалгоритм – способ формирования шифра замены над большим алфавитом. Требования к длине ключа и размерности преобразуемого блока данных. Рассеивание и перемешивание. Базовые шифрующие преобразования (линейные и нелинейные преобразования, инволюции). Блочные композиционные и итеративные шифры. Основные принципы разработки композиционных шифров. Основные схемы итеративных шифров (схема Фейстеля и ее обобщения). Режимы использования блочных шифров. Стандарты криптографической защиты информации ведущих государств (DES, ГОСТ 28147-89 и др.). Двойной и тройной DES. Подстановочно-перестановочная сеть. Rijndael – стандарт криптографической защиты информации XXI века.

*Раздел 5. «Принципы построения и реализации криптографических алгоритмов поточных шифров».*

Основные принципы разработки поточных шифров. Случайные и псевдослучайные последовательности: свойства, принципы и методы их построения. Генераторы псевдослучайных последовательностей и способы оценки их криптографических свойств.

Механические, электромеханические и электронные шифраторы. Синхронные и самосинхронизирующиеся поточные шифры. Регистры сдвига с обратной связью. Линейные рекуррентные последовательности.

*Раздел 6. «Асимметричные криптосистемы».*

Однонаправленные функции. Основные идеи построения криптосистем с открытыми ключами. Примеры асимметричных криптосистем: RSA, схема Эль-Гамаля. Применение асимметричных криптосистем: шифрование, электронная цифровая подпись (ЭЦП), открытое распределение ключей Диффи-Хеллмана. Генерация ключей для асимметричных криптосистем. Длины ключей. Аутентификация ключей.

*Раздел 7. «Криптографические функции хэширования и контроль целостности информации».*

Модель угроз для асимметричных криптосистем. Практическое применение асимметричных криптосистем. Гибридные криптосистемы. Функции хэширования. Определение хэш-функции. Примеры хэш-функций (MD4, MD5, SHA-1, ГОСТ Р 34.11-94). Построение функций хэширования на основе блочных шифров. Построение шифров на основе функций хэширования. Хэш-функции с ключом. Модель угроз для хэш-функций.

*Раздел 8. «Криптографические протоколы»*

Понятие криптографического протокола, определения. Простейшие протоколы: передача шифрованного трафика (SKIP, IPSEC ESP), аутентификация партнера (симметричные алгоритмы, асимметричные алгоритмы, их преимущества и недостатки), аутентификация

источника данных (IPSEC AH), выработка сеансового ключа. Распространенные протоколы: ЭЦП, битовое обязательство, доказательства с нулевым разглашением, односторонние аккумуляторы. Модель угроз для протоколов. Атаки: человек-посередине, атаки с заданным открытым текстом или шифртекстом. Примеры взлома протоколов.

**Раздел 3. Обеспечение учебных занятий**

**3.1. Методическое обеспечение**

**3.1.1 Методические указания по освоению дисциплины**

Успешное освоение дисциплины возможно благодаря посещению лекций, участию в обсуждении вопросов, подготовленных к занятию, самостоятельной работе, включающей в себя чтение специальной литературы по разделам темы, подготовка презентаций по тематике курса.

**3.1.2 Методическое обеспечение самостоятельной работы**

Самостоятельная работа обучающихся в рамках данной дисциплины является важным компонентом обучения, предусмотренным компетентностно-ориентированным учебным планом и рабочей программой учебной дисциплины.

Настоящей программой предусмотрены формы самостоятельной работы с использованием методических материалов.

**3.1.3 Методика проведения текущего контроля успеваемости и промежуточной аттестации и критерии оценивания**

Экзамен проводится в устной форме. Билет содержит 2 вопроса, на подготовку к ответу в аудитории отводится 1 академический час. В ходе беседы по вопросам преподаватель вправе задавать дополнительные вопросы и вопросы на смежные темы.

Экзамен допустимо проводить в удалённой форме средствами видеоконференцсвязи. По желанию преподавателя на экзамен допустимо приглашать других преподавателей с квалификацией не ниже изложенной в п. 3.2.1 как для независимого оценивания ответов обучающихся, так и для коллегиального. В последнем случае оценка за экзамен ставится на основании усреднения оценок каждого принимающего. В спорных ситуациях преподаватель, ведущий дисциплину, имеет право принятия окончательного решения.

Критерии выставления оценок за каждый вопрос:

* 50 баллов ставится за полностью раскрытый теоретический материал и правильные ответы на дополнительные вопросы преподавателя. В болонской шкале оценка может быть скорректирована в ту или иную сторону с учетом малозначительных погрешностей изложения или, напротив, углубленного изложения материала.
* 40 баллов ставится за изложенный теоретический материал вопроса (возможно с помощью наводящих подсказок преподавателя).
* 20 баллов ставится за знание основ тематики вопроса.
* 0 баллов выставляется, если обучающийся не может продемонстрировать знание основ тематики вопроса.

Баллы, полученные за ответ по каждому вопросу, суммируются, сумма баллов считается итоговым процентом выполнения. Далее применяется следующее правило выставления оценки:

|  |  |  |
| --- | --- | --- |
| Итоговый процент  выполнения, % | Оценка СПбГУ при  проведении экзамена | Оценка  ECTS |
| 90-100 | отлично | A |
| 80-89 | хорошо | B |
| 70-79 | хорошо | C |
| 61-69 | удовлетворительно | D |
| 50-60 | удовлетворительно | E |
| менее 50 | неудовлетворительно | F |

**3.1.4 Методические материалы для проведения текущего контроля успеваемости и промежуточной аттестации (контрольно-измерительные материалы, оценочные средства)**

*Примерный краткий перечень вопросов к зачету.*

1. Симметричные криптосистемы и криптосистемы с открытым ключом. Исторические шифры. Шифр замены, шифр сдвига. Стеганография.
2. Поточные шифры.
3. Блочные шифры. Алгоритм DES.
4. Блочные шифры. Алгоритм AES (Rijndael).
5. Блочные шифры. ГОСТ 28147-89.
6. Блочные шифры. Blowfish
7. Блочные шифры. Threefish
8. Режимы работы симметричных алгоритмов. Режимы ECB, CBC, OFB, CFB.
9. Распределение ключей для симметричных алгоритмов. Протоколы широкоротой лягушки, Нидхейм-Шредера. BAN логика.
10. Распределение ключей для симметричных алгоритмов. Протоколы широкоротой лягушки, Отвэй-Риса, Цербер. BAN логика.
11. Криптография с открытым ключом. Математические задачи, на которых она основывается.
12. Криптография с открытым ключом. Алгоритм RSA.
13. Криптография с открытым ключом. Эль-Гамаль.
14. Криптография с открытым ключом. Алгоритм Рабина.
15. Распределение ключей с помощью криптографии с открытым ключом. Алгоритм Диффи-Хэлмана и использование RSA для передачи ключей.
16. Цифровые подписи. Использование симметричной криптографии, криптографии с открытым ключом и хэш-функции для создания цифровой подписи. Digital Signature Algorithm.
17. Однонаправленные хэш-функции, метод Д.Р.
18. Хэш-функции. MD-5.
19. Хэш-функции. ГОСТ Р34.11-94.
20. Подпись ГОСТ Р34.10-2001.
21. Контрольная сумма.
22. Слепые подписи, одновременная подпись контракта.
23. Специальные алгоритмы для протоколов, раскрытие секретов все или ничего.
24. Удостоверение подлинности.
25. Длина ключа для симметричного и ассиметричного шифрования.
26. Криптоанализ, безопасность алгоритмов.

**3.1.5 Методические материалы для оценки обучающимися содержания и качества учебного процесса**

Для оценки обучающимися содержания и качества учебного процесса применяется анкетирование в соответствии с методикой и графиком, утвержденными в установленном порядке

**3.2. Кадровое обеспечение**

**3.2.1 Образование и (или) квалификация штатных преподавателей и иных лиц, допущенных к проведению учебных занятий**

К чтению лекций привлекаются преподаватели, имеющие базовое образование и/или ученую степень, соответствующую профилю преподаваемой дисциплины.

**3.2.2 Обеспечение учебно-вспомогательным и (или) иным персоналом**

Не требуется.

**3.3. Материально-техническое обеспечение**

**3.3.1 Характеристики аудиторий (помещений, мест) для проведения занятий**

Стандартно оборудованные лекционные аудитории для проведения интерактивных лекций: видеопроектор, экран.

**3.3.2 Характеристики аудиторного оборудования, в том числе неспециализированного компьютерного оборудования и программного обеспечения общего пользования**

Не предусмотрено.

**3.3.3 Характеристики специализированного оборудования**

Не предусмотрено.

**3.3.4 Характеристики специализированного программного обеспечения**

Не предусмотрено.

**3.3.5 Перечень и объёмы требуемых расходных материалов**

Фломастеры цветные, губки, бумага формата А3 (для блокнота-доски), канцелярские товары в объеме, необходимом для организации и проведения занятий по заявкам преподавателей, подаваемым в установленные сроки, доступ преподавателя и обучающихся к в компьютерные классы.

**3.4. Информационное обеспечение**

**3.4.1 Список обязательной литературы**

1. Н. Смарт. Криптография. Москва: Техносфера, 2005. 528 с. ISBN 5-94836-043-12.
2. Крук, Е. А., Линский Е.М. Криптография с открытым ключом. Кодовые системы: Учебное пособие. СПб.: РИО ГУАП, 2004. - 52 с.
3. Шнайер, Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. - 815 с.
4. Чмора, А. Л. Современная прикладная криптография. М.: Гелиос АРВ, 2002. 244 с.
5. Виноградов И.М. Основы теории чисел. Лань, 2009. <http://e.lanbook.com/view/book/46/>
6. Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. Лань, 2011. <http://e.lanbook.com/view/book/1540/>

**3.4.2 Список дополнительной литературы**

1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography <http://cacr.uwaterloo.ca/hac/>
2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. ДМК Пресс, 2008. 448 с. <http://e.lanbook.com/view/book/3027/>
3. Ф.П. Брукс "Мифический человеко-месяц", 2-е изд., СПб: Символ-плюс, 2001.
4. В.Н. Петров, "Информационные системы", Спб: Питер, 2006. 688с.
5. Джошуа Кериевски. Рефакторинг с использованием шаблонов. Refactoring to Patterns. Изд-во: Вильямс, 2006 г., 400 с.
6. С. Макконнелл. Совершенный код. Code Complete. Практическое руководство по разработке программного обеспечения. Изд-во: Питер, 2010 г., 896 стр.
7. Крэг Ларман. Применение UML 2.0 и шаблонов проектирования. Введение в объектно-ориентированный анализ, проектирование и итеративную разработку. Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development. Изд-во: Вильямс, 2013 г., 736 с.
8. Дж. Гринфилд, К. Шорт, С. Кук, С. Кент. Фабрики разработки программ. Потоковая сборка типовых приложений, моделирование, структуры и инструменты. Software Factories: Assembling Applications with Patterns, Models, Frameworks, and Tools. Изд-ва: Диалектика, Вильямс, 2007г., 592 с.
9. Собел Марк Г. Linux. Администрирование и системное программирование. Practical Guide to Linux Commands, Editors, and Shell Programming Изд-во: Питер; 2011 г., 880с.
10. Борисов В., Круглов В., Федулов А. Нечеткие модели и сети. Изд-во: Горячая Линия - Телеком, 2012 г., 284 с.

**3.4.3 Перечень иных информационных источников**

1. <https://www.pgpru.com/>
2. http://microsat.sm.bmstu.ru/e-library/Books/TheMythicalManMonth\_rus/The% 20Mythical%20Man-Month.pdf Ф.П. Брукс "Мифический человеко-месяц"
3. http://rutracker.org/forum/viewtopic.php?t=4342826 С. Макконнелл. Совершенный код.
4. http://html-kod.ru/docs/index-6074.html Р. Хантер "Основные концепции компиля-торов"
5. http://www.intuit.ru/studies/courses/607/463/info А. Барский Введение в нейронные сети.
6. http://www.intuit.ru/studies/courses/1053/150/info Кейт ДжонсБредли ДжонсонМайк Шема Инструментальные средства обеспечения безопасности.
7. В. В. Корнеев, А. Ф. Гареев, С. В. Васютин, В. В. Райх. Базы данных. Интеллектуальная обработка информации. М.: Нолидж, 2003. – 400 с.
8. Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайню Алгоритмы. Построение и анализ. Изд. 2-е. Introduction To Algorithms. Изд-во: Вильямс, 2007 г., 1296 с.
9. Э. Гамма, Р. Хелм, Р. Джонсон, Дж. Влиссидес. Приемы объектно-ориентированного проектирования. Паттерны проектирования. Design Patterns: Elements of Reusable Object-Oriented Software. Изд-во: Питер, 2007 г., 366 с.
10. М. Фаулер. UML. Основы. UML Distilled. Изд-тво: Символ-Плюс, 2006г., 192 с.
11. Б. Шнейдерман "Психология программирования", М.: Радио и связь, 1984. 304 с.
12. Э. Дейкстра "Дисциплина программирования", М., Мир, 1978. 275 с.
13. T. De Marco, T. Lister "Peopleware: Productive Projects and Teams", 2nd ed., 1999. 264 p
14. В. И. Грекул. "Теория информационных систем", <http://www.intuit.ru/department/itmngt/theoryis/>

**Раздел 4. Разработчики программы**

Левина Алла Борисовна, доцент кафедры ИАС СПбГУ, ablevina@itmo.ru