Программа учебной дисциплины: Программирование алгоритмов защиты информации

Утверждена
Кафедрой компьютерной безопасности
МИЭМ НИУ ВШЭ
Протокол № 1 от «31» августа 2018 г.

Автор	Нестеренко А.Ю. (anesterenko@hse.ru)
Число кредитов	4
Контактная работа (час.)	70
Самостоятельная работа (час.)	82
Курс	4 курс
Формат изучения дисциплины	Без использования онлайн курса

I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Целью освоения дисциплины является формирование у студентов следующих навыков (согласно п.4.4 ФГОС ВПО), необходимых для решения предусмотренных программой по направлению подготовки10.05.01 «Компьютерная безопасность» профессиональных задач:

- обоснование и выбор рационального решения по уровню обеспечения информационной безопасности с учетом заданных требований;
- сопровождение разработки технического и программного обеспечения систем и средств информационной безопасности;
- выполнение экспериментально-исследовательских работ при проведении сертификации средств защиты и анализ результатов;
- приемка и освоение программно-аппаратных средств защиты информации;
- составление инструкций по эксплуатации программно-аппаратных средств защиты информации;

В результате освоения дисциплины студент должен
знать:

- алгоритмы, реализующие основные операции с большими целыми числами и вычетами по модулю целого числа - операции сложения, вычитания, умножения, деления с остатком, взятия обратного элемента;
- алгоритмы, реализующие операции сложения и удвоения в группе точек эллиптической кривой, алгоритмы вычисления кратной точки эллиптической кривой;
- алгоритмы умножения матриц;
- алгоритмы эффективного нахождения состояний линейных регистров сдвига;
- способы реализации криптографических функций хеширования, определяемых национальными и зарубежными стандартами;
- алгоритмы вычисления имитовставки;

- способы реализации алгоритмов блочного шифрования, определяемых национальными и зарубежными стандартами;
- алгоритмы выработки и проверки электронной подписи.

уметь:

- разбирать исходные коды программ, реализующих известные криптографические алгоритмы;
- создавать программные реализации заданных криптографических алгоритмов;
- проводить верификацию разработанного программного обеспечения и оценку соответствия заданным требованиям по безопасности;
- разрабатывать документацию на программное обеспечение в соответствии с существующими требованиями.

иметь навыки (приобрести опыт):

- разработки программного обеспечения в области защиты информации в соответствии с заданными требованиями;
- создания документации и системы тестирования разработанного программного обеспечения;
- доказательства корректности разработанного программного обеспечения.

В результате освоения дисциплины студент осваивает следующие компетенции (согласно разделу 5 ФГОС ВПО):

- общекультурные: ОК-1, ОК-2, ОК-6, ОК-8;
- профессиональные: ПК-1, ПК-2, ПК-3, ПК-5, ПК-8, ПК-9, ПК-17, ПК-22, ПК-35, а также ПСК-2.3, ПСК-2.7.

Настоящая дисциплина относится к блоку дисциплин, читаемых в ходе 4 курса обучения в специалитете по направлению 10.05.01 «Компьютерная безопасность».

Для успешного освоения настоящей учебной дисциплины, студенты должны владеть следующими знаниями и навыками:

- знанием школьной программы;
- основными понятиями алгебры, теории конечных групп, колец и полей;
- основными понятиями алгоритмической теории чисел;
- знанием и навыками применения языков программирования C и C++;
- базовыми знаниями об операционных системах;
- базовыми знаниями о сетевых технологиях;
- базовым знанием технического английского языка;
- навыками поиска информации в сети Интернет;
- базовыми навыками разработки технической документации.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

- криптографические методы защиты информации;
- криптографические протоколы;
- теоретико-числовые методы в криптографии;
- методы алгебраической геометрии в криптографии,
- научный семинар,
- а также при написании итоговой выпускной квалификационной (дипломной)

работы.

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема 1. Основные языки и средства разработки программного обеспечения в области защиты информации;

Тема 2. Существующие нормативные документы в области средств защиты информации;

Тема 3. Система лицензирования средств защиты информации в Российской Федерации;

Тема 4. Алгоритмы сложения, вычитания, умножения и деления с остатком для больших целых чисел;

Тема 5. Примеры программных реализаций из распространенных библиотек с открытым исходным кодом;

Тема 6. Преобразование Монтгомери для оптимизации вычислений в конечных полях простой характеристики;

Тема 7. Алгоритм Баррета для приведения по модулю простого числа;

Тема 8. Группа точек эллиптической кривой: операции сложения и удвоения точек на эллиптической кривой, операция вычисления кратной точки и ее оптимизация;

Тема 9. Представления эллиптических кривых в формах Вейерштрасса, Монтгомери, Якоби, Гессе и Эдвардса; основные различия и области применения;

Тема 10. Операции в конечных полях малой характеристики; оптимизация вычислений для полей характеристики два; примеры программных реализаций из библиотек с открытым исходным кодом.

Тема 11. Матрицы; операции умножения матриц и умножения матрицы на вектор; алгоритмы вычисления ранга матрицы и обращения матрицы; MDS-матрицы и способы их генерации;

Тема 12. Линейные регистры сдвига; построение регистров максимального периода; алгоритмическая связь линейных регистров сдвига с умножением матрицы на вектор; примеры эффективных программных реализаций;

Тема 13. Перестановки на конечных множествах; построение перестановок с заданными свойствами; эффективная реализация перестановок для конечных полей характеристики два.

Тема 14. Методы разработки и отладки программного обеспечения;

Тема 15. Методы совместной разработки программного обеспечения;

Тема 16. Методы документирования программного обеспечения;

Тема 17. Методы доказательства корректности разработанного программного обеспечения; написание системы тестов;

Тема 18. Практические занятия по реализации поставленных задач;

Тема 19. Практические занятия по отладке и тестированию поставленных задач.

Тема 20. Алгоритмы поточного шифрования информации; примеры поточных шифров - алгоритмы rc4, a5 и grain128.

Тема 21. Алгоритм блочного шифрования гост 28147-89 (магма); ключевая система алгоритма гост 28147-89, слабые ключи алгоритма;

Тема 22. Алгоритм блочного шифрования гост р 34.12-2005 (кузнечик); описание различных принципов реализации алгоритма;

Тема 23. Алгоритм блочного шифрования aes; использование аппаратных инструкций архитектуры intel для реализации алгоритма aes;

Тема 24. Алгоритмические методы защиты ключевой информации, используемой в алгоритмах блочного шифрования;

Тема 25. Режимы использования блочных шифров (простая замена, простая замена с зацеплением, режимы гаммирования);

Тема 26. Связь блочных шифров с поточными шифрами;

Тема 27. Алгоритмы выработки имитовставки;

Тема 28. Режим выработки имитовставки для блочных шифров согласно гост р 34.13-2015);

Тема 29. Режим работы блочных шифров с возможностью аутентификации сообщений (одновременной выработкой имитовставки);

Тема 30. Режим работы блочных шифров с регулярным изменением ключевой информации (режим acpkm);

Тема 31. Функции хеширования; алгоритм гост р 34.11-94 (с использованием гост 28147-89);

Тема 32. Функция хеширования гост р 34.11-2012 (стрибог);

Тема 33. Функция хеширования keccak (стандарт fips 180-3);

Тема 34. Алгоритмы выработки имитовставки на основе бесключевых функций хеширования; алгоритм hmac;

Тема 35. Алгоритмы выработки и проверки электронной подписи; стандарт гост р 34.10-2012;

Тема 36. Асимметричные алгоритмы шифрования; гибридные схемы шифрования;

Тема 37. Инфраструктура открытых ключей; стандарты asn.1 и x.509; особенности применения инфраструктуры открытых ключей в российской федерации.

Тема 38. Практические занятия по реализации криптографических преобразований;

Тема 39. Сдача окончательной (годовой) программной реализации.

III. ОЦЕНИВАНИЕ

Формы контроля:

Тип контроля	Форма контроля	4 курс				Примечания
		1 модуль	2 модуль	3 модуль	4 модуль	

Текущий	Курсовая работа			*		
	Домашняя работа	*	*	*	*	
Итоговый	Экзамен в устной форме				*	

Промежуточная программная реализация оценивается отдельной оценкой по десятибальной шкале, из которых

- за разработанную самостоятельно студентом программную реализацию - максимум 4 балла,
- разработку документации по используемой внешней библиотеке и ее функциям - максимум 2 балла,
- описание реализации собственного алгоритма - максимум 2 балла,
- описание методов доказательства корректности разработанной реализации - максимум 2 балла.

В случае плагиата - предоставления чужой программной реализации или невозможности обосновать, что данная программная реализация написана студентом самостоятельно, проставляется общая оценка - 0 баллов.

Оценка, полученная студентом за промежуточную программную реализацию, является накопленной оценкой Q_1 по дисциплине «Программирование алгоритмов защиты информации».

Указанные выше значения баллов являются действительными до окончания второго модуля дисциплины. В случае, если студент не предоставляет промежуточную программную реализацию до окончания второго модуля, ему проставляется накопленная оценка 0 баллов.

К окончанию четвертого модуля студент должен предоставить итоговую программную реализацию. Оценка итоговой программной реализации Q_2 выставляется по десятибальной системе, из которых

- за разработанную самостоятельно студентом программную реализацию - максимум 6 баллов;
- описание реализации криптографического алгоритма – максимум 2 балла,
- доказательство корректности разработанной реализации – максимум 2 балла.

В случае плагиата - предоставления чужой программной реализации или невозможности обосновать, что данная программная реализация написана студентом самостоятельно, проставляется общая оценка - 0 баллов.

Итоговая оценка Q по предмету определяется из соотношения $Q = 0.5*Q_1 + 0.5*Q_2$, в котором округление происходит в меньшую сторону, например, величина $Q = 3.5$ дает студенту 3 балла.

В случае, если студент не может получить положительную оценку по предмету, то есть набрать 4 и более балов, назначается пересдача. В ходе пересдачи студент должен предъявить заданную ему итоговую программную реализацию и отчетные материалы.

Способ проставления оценки за пересдачу совпадает с изложенным ранее.

В случае неуспешной пересдачи назначается комиссия. На комиссии может быть отменена накопленная оценка, а также поставленная итоговая задача. Приемной комиссией студенту может быть поставлена новая задача (из тем, рассматривавшихся в учебной дисциплине), которую он должен реализовать за время пересдачи. Время решения поставленной задачи не должно превышать двух часов.

IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

Контроль знаний студентов производится по окончании второго и четвертого модулей.

По окончании второго модуля студентом подготавливается промежуточная отчетная программная реализация. Цель промежуточной программной реализации заключается в получении *практических навыков использования внешнего программного обеспечения* и разработки с его помощью заданных алгоритмов защиты информации.

В рамках промежуточной программной реализации студентам предлагается выполнить следующие задания:

- самостоятельно реализовать определенный (согласованный) преподавателем алгоритм, используя при этом одну или несколько существующих библиотек с открытым исходным кодом.
- обосновать и реализовать систему тестирования и доказательства корректности выполнения разработанной программной реализации;
- подготовить отчет (в письменной форме) о проделанной работе, включающий в себя: описание реализованного алгоритма, используемые математические объекты, описание используемых библиотечных функций, описание методов тестирования разработанного программного обеспечения.

Отчетные материалы по промежуточной программной реализации должны быть оформлены в виде отдельного отчета (проекта) и представлять собой отпечатанный на принтере документ формата а4 на русском или английском языке.

При подготовке отчета желательным является использование правил оформления документов и исходных текстов программ, принятых в Единой системе программной

документации (ЕСПД), регламентируемой национальными стандартами Российской Федерации.

Выбор задачи для промежуточной программной реализации должен быть произведен студентом в ходе первого модуля.

В качестве примеров задач для промежуточной программной реализации могут выступать:

- реализация алгоритма вычисления кратной точки эллиптической кривой, заданной в форме Эдвардса, с использованием свободно распространяемой библиотеки libgcrypt;
- реализация алгоритма вычисления заданного состояния линейного регистра сдвига, используя вычисления с сопровождающей матрицей и свободно распространяемую библиотеку libgmp;

По окончании четвертого модуля студентом сдается окончательная (итоговая) программная реализация. Цель итоговой программной реализации заключается в получении практических навыков исследования и *модернизации существующего программного обеспечения* в области защиты информации.

В рамках итоговой программной реализации студентам предлагается выполнить следующие задания:

- самостоятельно реализовать определенный (согласованный) преподавателем криптографический алгоритм, используя при этом существующие функции заданного программного обеспечения (средства);
- встроить реализованный алгоритм в заданное программное средство;
- обосновать и реализовать систему тестирования и доказательства корректности выполнения модернизированного программного средства;
- подготовить отчет (на русском или английском языке) о проделанной работе, включающий в себя: описание реализованного алгоритма, включая используемые математические объекты, описание методов встраивания реализованного алгоритма, описания используемых функций, описание методов тестирования разработанного программного обеспечения.

Отчетные материалы по итоговой программной реализации должны быть оформлены в виде отдельного отчета (проекта) и представлять собой отпечатанный на принтере документ формата а4 на русском или английском языке. Требования к подготовке отчетных материалов совпадают с требованиями к отчету по промежуточной программной реализации.

Выбор студентом задачи для итоговой программной реализации должен быть произведен в ходе третьего модуля.

В качестве примеров задач для итоговой программной реализации могут выступать:

- реализация и встраивание в существующее программное средство алгоритма бесключевого хеширования Keccak;
- реализация и встраивание в существующее программное средство схемы электронной

подписи ГОСТ Р 34.10-2012;

- встраивание в ядро операционной системы Linux программного модуля, реализующего алгоритм блочного шифрования, регламентированный ГОСТ Р 34.12-2015.

V. РЕСУРСЫ

1. Основная литература

- С. Гребнев, А. Нестеренко, А. Пугачев. «Методы программной реализации средств криптографической защиты информации в Linux», 2016.
- А. Лось, А. Нестеренко, М.Рожков. «Криптографические методы защиты информации». – Юрайт, 2017.

2. Дополнительная литература

- Р 1323565.1.012-2017. Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. – Стандартинформ. 2017.
- Роберт Лав. Linux. Системное программирование. – Спб:Питер. – 2008. – 416с.
- Роберт Лав. Разработка ядра Linux. – Вильямс. – 2008. – 448с.
- С. Зубков. Assembler для DOS, Windows и Unix. –М.:ДМК Пресс. – 2015. –638с.

3. Программное обеспечение

№ п/п	Наименование	Условия доступа
1.	Microsoft Windows 7 Professional RUS Microsoft Windows 10 Microsoft Windows 8.1 Professional RUS	Из внутренней сети университета (договор)
2.	Microsoft Office Professional Plus 2010	Из внутренней сети университета (договор)

4. Профессиональные базы данных, информационные справочные системы, интернет-ресурсы (электронные образовательные ресурсы)

№ п/п	Наименование	Условия доступа
1.	Электронно-библиотечная система Юрайт	URL: https://biblio-online.ru/
2.	Открытое образование	URL: https://openedu.ru/

5. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

– ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением.

Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены компьютерами, с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде НИУ ВШЭ.