Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)»

УТВЕРЖДЕНО
Директор физтех-школы аэрокосмических технологий
С.С. Негодяев

Рабочая программа дисциплины (модуля)

по дисциплине:	Информационная безопасность и защита информации
по направлению:	Системный анализ и управление
профиль подготовки:	Системный анализ и управление в технических, экономических и социальных системах
	Физтех-школа Аэрокосмических Технологий
	кафедра логистических систем и технологий
курс:	4
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Дифференцированный зачет

Аудиторных часов: 30 всего, в том числе:
- лекции: 30 час.
- семинары: 0 час.
- лабораторные занятия: 0 час.

Самостоятельная работа: 15 час.

Всего часов: 45, всего зач. ед.: 1

Программу составил: А.И. Колыбельников, ассистент

Программа обсуждена на заседании кафедры логистических систем и технологий 03.06.2020

Аннотация

В курсе рассматриваются основные понятия и методы организации защиты информации. Прежде всего рассматриваются разделы криптографии, технических методов защиты информации, нормативно-правовых подходов к защите информации, организации систем защиты информации. Рассматриваются теория Шеннона, принципы Керкгоффса, модель Белла-Лападулы.

Курс содержит в себе обсуждение общих подходов к управлению рисками, средств противодействия взлому компьютерных систем, систем защиты от утечек информации.

1. Цели и задачи

Цель дисциплины

- формирование целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты компьютерной информации, используемых в современных криптосистемах, знакомство с законодательством и стандартами в этой области.

Задачи дисциплины

- сформировать взгляд на криптографию и защиту информации как на систематическую научно-практическую деятельность, носящую прикладной характер;
- изучить базовые теоретические понятия, лежащие в основе процесса защиты информации, сервисы и механизмы безопасности;
- изучить актуальные законодательные нормы в области защиты информации.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-3 Способен применять полученные знания, умения и навыки для решения типовых задач управления в технических системах	ОПК-3.1 Владеет основными понятиями и законами теории управления
ОПК-4 Способен применять типовые критерии оценки эффективности полученных результатов разработки систем управления и их внедрения в производственной и непроизводственной сферах	ОПК-4.1 Строит и использует на практике типовые критерии оценки эффективности полученных результатов разработки систем управления
	ОПК-4.2 Анализирует и определяет оптимальные критерии оценки эффективности полученных результатов разработки систем управления

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- правовые основы защиты компьютерной информации;
- математические основы криптографии;
- организационные, технические и программные методы защиты, информации в современных компьютерных системах и сетях;
- стандарты, модели и методы шифрования;
- методы идентификации пользователей, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей;
- методы передачи конфиденциальной информации по каналам связи, методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных).

уметь:

- применять известные методы и средства поддержки информационной безопасности в компьютерных системах;
- проводить сравнительный анализ;
- выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах.

владеть:

- навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации;
- навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации, алгоритмы простановки и проверки электронной цифровой подписи, алгоритмы хэш-функций, алгоритмы генерации псевдослучайных последовательностей чисел.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Основные понятия и определения защиты информации	3			1
2	Правовые основы защиты компьютерной информации	3			2
3	Технические средства защиты информации	3			1
4	Симметричные и поточные методы шифрования	3			2
5	Асимметричные методы шифрования	3			1
6	Генерация случайных чисел, разделение секрета	3			2
7	Методы идентификации пользователей, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей	6			3
8	Методы передачи конфиденциальной информации по каналам связи	6			3
Итого часов		30			15
Подготовка к экзамену		0 час.			
Общая трудоёмкость		45 час., 1 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 7 (Осенний)

1. Основные понятия и определения защиты информации

Теоретические основы, введение в работы Шеннона по защите информации. Использование математического аппарата теории информации в качестве теоретического базиса защиты информации. Понятие об абсолютно защищённых системах. Краткий исторический обзор.

2. Правовые основы защиты компьютерной информации

Система законодательства в области защиты информации – Конституция РФ, федеральные законы, приказы Президента РФ, постановления Правительства РФ, отраслевые НПА. Защита персональных данных, защита конфиденциальных сведений, защита банковской тайны. Обзор федерального и международного законодательства.

3. Технические средства защиты информации

Средства криптографической защиты информации. Нормативные требования к различным техническим средствам защиты. Основные подходы к проектированию и использованию. Межсетевые экраны, системы обнаружения вторжений, антивирусы, системы AAA, SIEM, SOAR.

4. Симметричные и поточные методы шифрования

Блоковые и потоковые шифры. Генераторы криптографически стойких псевдослучайных последовательностей.

5. Асимметричные методы шифрования

Обеспечение конфиденциальности и целостности информации с использованием криптосистем RSA, El Gamal и криптосистем на основе эллиптических кривых. Гомоморфное шифрование. Протоколы распространения ключей. Криптографически стойкие хеш-функции. Государственный стандарт «СТРИБОГ». Семейство хэш-функций SHA.

6. Генерация случайных чисел, разделение секрета

Создание случайных последовательностей, управление ключами, алгоритм Diffie-Hellman, управление ключей при помощи PKI, протокол Шамира, протокол Блекли.

7. Методы идентификации пользователей, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей

Методы идентификации пользователей, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей. Протокол TLS, протокол IPSec.

8. Методы передачи конфиденциальной информации по каналам связи

Методы передачи конфиденциальной информации по каналам связи, методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных). Использование электронных подписей, хешей, MAC.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

учебная аудитория, оснащенная компьютером и мультимедийным оборудованием (проектор, звуковая система).

6.Перечень рекомендуемой литературы

Основная литература

1. Защита информации [Текст] : учеб. пособие для вузов / Э. М. Габидулин, А. С. Кшевецкий, А. И. Колыбельников ; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т .— М. : МФТИ, 2011 .— 262 с.
2. Шнайер Брюс « Прикладная криптография»
3. Гошко С.В. Энциклопедия по защите от вирусов.- М.: Солон-Пресс, 2004.-301с.

Дополнительная литература

1. Защита объектов и информации от технических средств разведки [Текст] : учеб. пособие для вузов / Ю. К. Меньшаков ; Рос. гос. гуманит. ун-т .— М. : Изд-во Рос. гос. гуманит. ун-та, 2002 .— 399 с.
1. Конеев И.Р.,Беляев А.В. Информационная безопасность предприятия.-СПб.:БХВ-Петербург,2003.-733с.-(
2. Нечаев В.И. Элементы криптографии.Основы теории защиты информации.-М.:Высшая школа,1999.-108.-
3. Панасенко С.П.,Батура В.П. Основы криптографии для экономистов:Учеб.пособие для вузов/Под ред.Л.Г.Гагариной.-М.:Финансы и статистика,2005.-173
4. Скляров Д.В. Искусство защиты и взлома информации. СПб.:БХВ-Петербург,2004.-276с
5. Соколов А.В.,Степанюк О.М. Шпионские штучки:Методы информационной защиты объектов и компьютерных сетей.- СПб.;М.:Полигон:АСТ,2000.-269с
6. Технологии в преступном мире:Компьютерные телекоммуникационные технологии/Авт.-сост.В.Н.Соколов.-Минск: Литература,1998.-511с.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

1. Федеральный портал «Российское образование»: http://www.edu.ru
2. Библиотека по естественным наукам Российской академии наук: http://benran.ru
3. Информационный портал: https://www.securitylab.ru/about.php
4. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): https://fstec.ru

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

В образовательном процессе могут использоваться при необходимости дистанционные занятия и вебинары с использованием коммуникационного программного обеспечения Zoom, сервиса видеотелефонной связи Google Meet, веб-сервиса Google Класс.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Приступая к изучению дисциплины, необходимо в первую очередь ознакомиться содержанием дисциплины. Лекции имеют целью дать систематизированные основы научных знаний об основах защиты информации, о методах, технологиях и технических средствах, применяемых в процессе защиты.

При изучении и проработке теоретического материала для студентов необходимо:

- повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные литературные источники.

Работа с учебной и научной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на лекционных занятиях, к зачету. Она включает проработку лекционного материала – изучение рекомендованных источников и литературы по тематике лекций. Конспект лекции должен содержать реферативную запись основных вопросов лекции, предложенных преподавателем схем (при их демонстрации), основных источников и литературы по темам, выводы по каждому вопросу. Конспект должен быть выполнен в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки. Конспекты научной литературы при самостоятельной подготовке к занятиям должны быть выполнены также аккуратно, содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

Руководство и контроль за самостоятельной работой студента осуществляется на практических занятиях и в форме индивидуальных консультаций.

ПРИЛОЖЕНИЕ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Системный анализ и управление
профиль подготовки: Системный анализ и управление в технических, экономических и социальных системах
Физтех-школа Аэрокосмических Технологий
кафедра логистических систем и технологий
курс: ~~4~~
квалификация: бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Дифференцированный зачет

Разработчик: А.И. Колыбельников, ассистент

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-3 Способен применять полученные знания, умения и навыки для решения типовых задач управления в технических системах	ОПК-3.1 Владеет основными понятиями и законами теории управления
ОПК-4 Способен применять типовые критерии оценки эффективности полученных результатов разработки систем управления и их внедрения в производственной и непроизводственной сферах	ОПК-4.1 Строит и использует на практике типовые критерии оценки эффективности полученных результатов разработки систем управления
	ОПК-4.2 Анализирует и определяет оптимальные критерии оценки эффективности полученных результатов разработки систем управления

2. Показатели оценивания компетенций

В результате изучения дисциплины «Информационная безопасность и защита информации» обучающийся должен:

знать:

- правовые основы защиты компьютерной информации;
- математические основы криптографии;
- организационные, технические и программные методы защиты, информации в современных компьютерных системах и сетях;
- стандарты, модели и методы шифрования;
- методы идентификации пользователей, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей;
- методы передачи конфиденциальной информации по каналам связи, методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных).

уметь:

- применять известные методы и средства поддержки информационной безопасности в компьютерных системах;
- проводить сравнительный анализ;
- выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах.

владеть:

- навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации;
- навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации, алгоритмы простановки и проверки электронной цифровой подписи, алгоритмы хэш-функций, алгоритмы генерации псевдослучайных последовательностей чисел.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Текущий контроль проводится в период аудиторной и самостоятельной работы студентов в установленные сроки по расписанию.

Оценка ответов на вопросы в процессе краткого (до 5 мин) выборочного устного опроса перед началом каждого практического занятия по материалам предыдущего занятия;

Примеры устных вопросов:

1) Стеганография
2) Конфиденциальность
3) Анонимность
4) Хеш-функция
5) Целостность

6) Цифровая подпись
7) Подпись Нюберга-Руэппеля
8) Криптоанализ
9) Атака на основе шифротекста
10) Атака на основе открытых текстов
11) Атака на основе подобранного открытого текста
12) Атака на основе адаптивно подобранного открытого текста
13) Атака на основе подобранного шифротекста
14) Атака на основе подобранного ключа
15) Атака на основе связанных ключей
16) Бандитский криптоанализ
17) Социальная инженерия (безопасность)
18) side-channel криптоанализ
19) Дифференциальный криптоанализ
20) Линейный криптоанализ
21) Перебор по словарю
22) Полный перебор
23) Радужная таблица
24) Человек посередине (атака)
25) Шифрование
26) Поточный шифр
27) Генератор псевдослучайных чисел
28) Регистр сдвига с линейной обратной связью
29) Линейный конгруэнтный метод
30) Метод Фибоначчи с запаздываниями
31) Регистр сдвига с линейной обратной связью
32) Регистр сдвига с обобщённой обратной связью
33) Генератор Макларена — Марсальи
34) Криптографически стойкий генератор псевдослучайных чисел
35) Симметричные криптосистемы
36) Блочный шифр
37) Сеть Фейстеля
38) Лавинный эффект
39) Режим шифрования
40) AEAD Режим
41) Асимметричные криптосистемы
42) Гомоморфное шифрование
43) Криптографическая стойкость
44) Абсолютная криптографическая стойкость
45) Латинский квадрат
46) Шифр Вернама
47) Постквантовая криптография
48) Алгоритм Евклида
49) Соотношение Безу
50) Расширенный алгоритм Евклида

Обучающийся должен проявить всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоить основную литературу и быть знакомым с дополнительной литературой, рекомендованной программой дисциплины, усвоить взаимосвязь основных понятий дисциплины, решать предложенные преподавателем задачи.

Критерии оценивания по устному опросу:

9-10 баллов : Выставляется, если обучающийся раскрыл содержание материала в объеме, предусмотренном программой, изложил материал грамотным языком в определенной логической последовательности, точно используя терминологию данного предмета как учебной дисциплины; отвечал самостоятельно без наводящих вопросов преподавателя; успешно ответил на тестовые задания, правильно и обоснованно решил ситуационные задачи, продемонстрировал умение заполнять медицинскую документацию (отчетные и учётные формы). Возможны одна – две неточности при освещении второстепенных вопросов или в выкладках, которые обучающийся легко исправил по замечанию преподавателя.

7-8 баллов: Выставляется, если ответ обучающегося удовлетворяет в основном требованиям на отметку «отлично», но при этом имеет место один из недостатков: допущены одна - две неточности при освещении основного содержания ответа, исправленные по замечанию преподавателя; допущены ошибка или более двух неточностей при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.

4-6 баллов: Выставляется в следующих случаях: неполно или непоследовательно раскрыто содержание материала, имеются ошибки при ответах на тесты, неточности в решении ситуационных задач, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала, определенного учебной программой дисциплины.

1-3 балла : Выставляется в случаях, если не раскрыто основное содержание учебного материала; обнаружено незнание или неполное понимание обучающимся большей или наиболее важной части учебного материала; допущены грубые ошибки при ответах на вопросы собеседования, неправильно решены ситуационные задачи, допущены ошибки в ответах на тесты, не продемонстрировано умение заполнения медицинской документации; допущены ошибки в определении понятий при использовании специальной терминологии в рисунках, схемах, выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

1) Защита персональных данных в РФ
2) Порядок импорта СКЗИ в РФ
3) Оценка защищенности web-сайта.
4) Уязвимости систем ДБО.
5) Генераторы случайных чисел и их применение.
6) Симметричные шифры – область применения, подходы к проектированию.
7) Электронная подпись – требования по обеспечению юридической значимости.
8) Проектирование системы защиты информации – основной подход.
9) Формирование технического задания на создание системы защиты информации персональных данных.
10) Формирование технического задания на создание системы защиты информации конфиденциальных сведений.
11) Формирование технического задания на создание системы защиты информации банковской тайны.
12) Основы безопасной разработки средств защиты информации.
13) Формирование технического задания на создание системы защиты информации платежной системы.
14) Поиск уязвимостей и их верификация.
15) Методика работы с уязвимостями.
16) Модель угроз.
17) Модель нарушителя.
18) Нормативное обеспечение проекта по защите информации.
19) Обязанности банка по защите информации клиента.
20) Порядок рассмотрения конфликтной ситуации с электронной подписью.
21) Методики генерации и управления паролями.
22) Криптографические протоколы – методика применения.
23) Порядок рассмотрения инцидента по утечке персональных данных в органах правопорядка.

24) Порядок рассмотрения инцидента по утечке банковской тайны в органах правопорядка.

25) Порядок рассмотрения инцидента по утечке конфиденциальных сведений в органах правопорядка.

26) Порядок действий при компрометации ключей.

27) Документооборот – обеспечение безопасности и юридической значимости.

28) Методы шифрования.

Примеры билетов на дифференцированном зачёте:

Билет 1.

1) Порядок рассмотрения инцидента по утечке конфиденциальных сведений в органах правопорядка.

2) Модель нарушителя.

Билет 2.

1. Основы безопасной разработки средств защиты информации.
2. Модель угроз.

Критерии оценивания

оценка «отлично (10)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины при ответе билета и ответе на вопросы по программе дисциплины;

оценка «отлично (9)» выставляется студенту, показавшему систематизированные, глубокие знания учебной программы дисциплины при ответе билета и ответе на вопросы по программе дисциплины;

оценка «отлично (8)» выставляется студенту, показавшему систематизированные, знания учебной программы дисциплины при ответе билета и ответе на вопросы по программе дисциплины;

оценка «хорошо (7)» выставляется студенту, если он твердо знает материал билета, грамотно и, по существу, излагает его, умеет применять полученные знания на практике, но допускает в ответе некоторые неточности;

оценка «хорошо (6)» выставляется студенту, если он знает материал билета, по существу, излагает его, умеет применять полученные знания на практике, но допускает в ответе много неточностей;

оценка «хорошо (5)» выставляется студенту, если он знает материал билета, излагает его, умеет применять полученные знания на практике, не допускает в ответе грубых ошибок;

оценка «удовлетворительно (4)» выставляется студенту если во время ответа билета он показал фрагментарный, характер знаний, недостаточно правильные формулировки базовых понятий, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения;

оценка «удовлетворительно (3)» выставляется студенту, если во время ответа билета он показал разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушение логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

оценка «неудовлетворительно (2-1)» выставляется студенту, если во время ответа билета, он показал, что не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Текущий контроль осуществляется в виде ответов на вопросы по темам занятий.

Промежуточный контроль проводится в форме дифференцированного зачёта – ответы на вопросы по билетам на темы дисциплины.

Оценка за текущий контроль учитывает оценку Отекущий.

Итоговая оценка учитывает оценку за текущий контроль Отекущий и оценку за работу непосредственно на зачете Одифф.зачет и рассчитывается по формуле:

Оитоговая=0.8* Одифф.зачет +0.5*Отекущий. Округляется до ближайшего целого.