

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

УТВЕРЖДЕНО
Проректор по учебной работе

А.А. Воронов

	Рабочая программа дисциплины (модуля)
по дисциплине:	Защита информации
по направлению:	Системный анализ и управление
профиль подготовки:	Управление инновациями в бизнесе
	Физтех-школа бизнеса высоких технологий
	кафедра информатики и вычислительной математики
курс:	4
квалификация:	бакалавр

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

Аудиторных часов: 30 всего, в том числе:

лекции: 0 час.

семинары: 30 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 60 час.

Всего часов: 90, всего зач. ед.: 2

Количество контрольных работ, заданий: 2

Программу составил: Т.Ф. Хирьянов, старший преподаватель

Программа обсуждена на заседании кафедры информатики и вычислительной математики 31.08.2023

Аннотация

В рамках данной дисциплины вы узнаете меры по обеспечению кибербезопасности на предприятии, научитесь выбирать необходимые инструменты и алгоритмы защиты информации в зависимости её критичности.

1. Цели и задачи

Цель дисциплины

- овладение студентами базовыми понятиями, стандартами, подходами и технологиями по обеспечению информационной безопасности, для их применения в реальных проектах.

Задачи дисциплины

- приобретение студентами навыков по обеспечению кибербезопасности на предприятии, способность выбирать необходимые инструменты и алгоритмы защиты информации в зависимости критичности информации, инфраструктуры потребностей организации по её защите.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-6 Способен применять математические, системно-аналитические, вычислительные методы и программные средства для решения прикладных задач в области создания систем анализа и автоматического управления и их компонентов	ОПК-6.3 Использует программные средства для разработки информационных систем
	ОПК-6.4 Осуществляет поиск необходимой информации в базах данных и информационных системах

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- основные понятия КБ и направления деятельности;
- законодательство, стандарты и спецификации в области КБ; виды тайн;
- подходы к организации комплексной защиты организации, а также тенденции их развития;
- типы системы комплексной защиты организаций и направления их использования;
- основные подходы и методы защиты данных;
- методы проведения аудита систем и ПО на КБ.

уметь:

- выявлять основные угрозы (уязвимости и риски); строить модели угроз и рисков;
- планировать работы по выполнению проектов, связанных с информационной безопасностью;
- управлять рисками информационной безопасности;
- обеспечивать защиту персональных данных и других видов тайн;
- организовывать защиты конфиденциальных документов.

владеть:

- навыками постановки задачи защиты информации в интересах компании, способами обеспечения кибербезопасности данных;
- навыками организации комплексной защиты информации;
- навыками донесения результатов оценки рисков и угроз и предлагаемых мер защиты.

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

	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.
--	---

№	Тема (раздел) дисциплины	Лекции	Семинары	Лаборат. работы	Самост. работа
1	Введение и обзор истории и современного состояния кибербезопасности.		6		12
2	Криптографическая защита.		6		12
3	Техническая защита.		6		12
4	Комплексная защита организации.		6		12
5	Нормативные руководящие документы, назначение и задачи информационной безопасности России		6		12
Итого часов			30		60
Подготовка к экзамену		0 час.			
Общая трудоёмкость		90 час., 2 зач.ед.			

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

Семестр: 7 (Осенний)

1. Введение и обзор истории и современного состояния кибербезопасности.

- Основные понятия КБ и направления деятельности. Актуальность и важность предмета. История КБ.
- Основные Угрозы (уязвимости и риски). Модели угроз и рисков. Теория игр и др. Каналы утечки. Вирусы, спам, фишинг, социальная инженерия, Современные проблемы информационно-психологического противоборства.
- Управление рисками
- Обзор норматив КБ в РФ, Банке, мире. Законодательство, стандарты и спецификации. Организационное обеспечение КБ.
- Обеспечение защиты Персональных данных.
- Виды тайн: государственная, коммерческая, банковская, ...
- АИБ и методы проведения аудита систем и ПО.

2. Криптографическая защита.

- Виды и история шифров. Симм., Асим, ЭЦП, хэш, «соль», Стеганография, ЦВЗ, ключи и сертификаты PKI;
- Уязвимости и методы взлома шифров. Полный перебор, частотный анализ, радужные таблицы.
- Основные направления использования криптографии в КБ. AAA (Authentication, Authorization, Accounting) аутентификация, авторизация, учёт (access logs)
- СКЗИ (ViPNet, КриптоПро, Верба)?
- Программно-аппаратные средства защиты от НСД

3. Техническая защита.

- Совр. Тех. средства ЗИ.
- Порядок проектирования СЗИ.
- Оценки защищенности СЗИ. Критерии определения безопасности компьютерных систем.
- Обеспечение высокой доступности.
- Основы ОС и безопасность ОС. (Windows & Linux).

- Основы сетевых протоколов и сетевая безопасность, стек протоколов TCP/IP, IPSec, SSL, TLS. Классификация основных типов сетевых атак; основные характеристики различных типов межсетевых экранов, анализ защищенности; принципы построения виртуальных частных сетей (VPN) + туннелирование, безопасность маршрутизаторов с использованием списков контроля доступа и возможностей по протоколированию событий.
- Основные уязвимости при написании кода, безопасный код, ООП в ИБ, DevSecOps, тестирование на безопасность.
- Основные уязвимости web-сайтов и web-сервисов, основы безопасной разработки вебсервисов, сайтов, распределенные атаки типа "отказ в обслуживании".
- Биометрия.
- Безопасность виртуальных и облачных технологий.
- Кибербезопасность BigData.
- BigData и AI для инфо безопасности.
- Порядок лицензирования деятельности в КБ

4. Комплексная защита организации.

- Политика и программа безопасности (Административный уровень)
- Основные классы мер процедурного уровня ИБ
- Принципы построения комплексных СЗИ
- Построение "демилитаризованных зон" (DMZ) для корпоративной сети
- системы обнаружения вторжений (IDS) для идентификации попыток вторжения
- Система предотвращения вторжений (IPS)
- Предотвращение утечек информации (DLP)
- управление информационной безопасностью и управление событиями безопасности (SIM+SEM=SIEM)
- Песочницы (sandbox) и ловушки (honeypots)
- Идентификация и аутентификация, управление доступом
- Протоколирование и аудит, шифрование, контроль целостности
- Планы бесперебойной работы, реализация бесперебойного электропитания и резервного копирования данных

5. Нормативные руководящие документы, назначение и задачи информационной безопасности России

- Обзор норматив КБ в РФ, в Банке, в мире.
- Российские и международные организации и стандарты.
- Законодательство, стандарты и спецификации. Организационное обеспечение КБ.
- Обеспечение защиты Персональных данных. Неприкосновенность частной жизни.
- Виды тайн: государственная, коммерческая, банковская, ...; и основные нормы.
- Законодательство в области интеллектуальной собственности
- Требования к защищенности автоматизированных систем.

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

- Учебная аудитория
- Проектор
- Маркерная доска
- Рабочие станции с подключением к Интернет
- Виртуальные машины (установленные локально или в облачной инфраструктуре)

6.Перечень рекомендуемой литературы

Основная литература

1. Криптографические методы защиты информации [Текст], учеб. пособие для вузов / С. М. Владимиров [и др.] , М., МФТИ, 2016

Дополнительная литература

1. Информационная безопасность [Текст] : учеб. пособие для вузов / М. М. Котухов, А. Н. Кубанков, А. О. Калашников ; М-во обр. и науки РФ ; Федеральное агентство по обр.; Моск. физико-техн. ин-т (гос. ун-т) ; Академия ИБС .— М. : Академия ИБС : МФТИ, 2009 .— 194 с.

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

1. <http://www.machinelearning.ru> – профессиональный информационно-аналитический ресурс, посвященный машинному обучению, распознаванию образов и интеллектуальному анализу данных.

2. <http://shad.yandex.ru> – сайт школы анализа данных Яндекса.

3.

http://www.machinelearning.ru/wiki/index.php?title=%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5_%28%D0%BA%D1%83%D1%80%D1%81_%D0%BB%D0%B5%D0%BA%D1%86%D0%B8%D0%B9%2C_%D0%9A.%D0%92.%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D1%86%D0%BE%D0%B2%29

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

На занятиях используются мультимедийные технологии, включая демонстрацию презентаций.

В процессе самостоятельной работы обучающихся предполагается использование таких программных средств, как WEKA, IPython Notebook и др.

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

Успешное освоение курса требует самостоятельной работы студента.

Самостоятельная работа включает в себя:

- проработку учебного материала (по учебной и научной литературе);
- подготовку к практическим занятиям, выполнение домашних теоретических и практических заданий;
- подготовку к дифференцированному зачёту.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Системный анализ и управление
профиль подготовки: Управление инновациями в бизнесе
Физтех-школа бизнеса высоких технологий
кафедра информатики и вычислительной математики
курс: 4
квалификация: бакалавр

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

Разработчик: Т.Ф. Хирьянов, старший преподаватель

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-6 Способен применять математические, системно-аналитические, вычислительные методы и программные средства для решения прикладных задач в области создания систем анализа и автоматического управления и их компонентов	ОПК-6.3 Использует программные средства для разработки информационных систем
	ОПК-6.4 Осуществляет поиск необходимой информации в базах данных и информационных системах

2. Показатели оценивания компетенций

В результате изучения дисциплины «Защита информации» обучающийся должен:

знать:

- основные понятия КБ и направления деятельности;
- законодательство, стандарты и спецификации в области КБ; виды тайн;
- подходы к организации комплексной защиты организации, а также тенденции их развития;
- типы системы комплексной защиты организаций и направления их использования;
- основные подходы и методы защиты данных;
- методы проведения аудита систем и ПО на КБ.

уметь:

- выявлять основные угрозы (уязвимости и риски); строить модели угроз и рисков;
- планировать работы по выполнению проектов, связанных с информационной безопасностью;
- управлять рисками информационной безопасности;
- обеспечивать защиту персональных данных и других видов тайн;
- организовывать защиты конфиденциальных документов.

владеть:

- навыками постановки задачи защиты информации в интересах компании, способами обеспечения кибербезопасности данных;
- навыками организации комплексной защиты информации;
- навыками донесения результатов оценки рисков и угроз и предлагаемых мер защиты.

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

С целью контроля освоения обучающимися учебного материала проводится устный опрос в начале занятия по теме прошлого занятия.

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

1. Основные направления деятельности по обеспечению Кибербезопасности
2. Защита информации в системе национальной безопасности Российской Федерации
3. Содержание нормативных правовых актов РФ, в Банке и в мире в сфере защиты информации
4. Стандарты и спецификации в области Кибербезопасности
5. Закон РФ "О персональных данных". Обеспечение защиты Персональных данных.
6. Виды тайн: государственная, коммерческая, банковская. Нормативные документы, отнесение, способы обеспечения защиты.
7. Основные категории угроз информационной безопасности объекта. Модели угроз и рисков. Теория игр и др. Каналы утечки
8. Основные виды вирусов и методы борьбы с ними
9. Защита от вредоносных программных воздействий, защита программ от изменений и контроль целостности, построение изолированной программной среды
10. Современные проблемы информационно-психологического противоборства. Социальная инженерия.
11. Методы воздействия при спаме и фишинге, основные правила противостояния

12. Управление рисками в информационной безопасности
13. Виды и история шифров. Симметричная и асимметричная криптография. Стойкость шифров.
14. Стеганография. Цифровые водяные знаки.
15. Электронная цифровая подпись, различные алгоритмы и их стойкость. Хэш, «соль», облачная ЭЦП.
16. Управление ключевой информацией и сертификатами; PKI.
17. Уязвимости и методы взлома шифров. Полный перебор, частотный анализ, радужные таблицы...
18. Основные направления использования криптографии в КБ. AAA (Authentication, Authorization, Accounting) аутентификация, авторизация, учёт (access logs)
19. Основные принципы построения программно-аппаратных комплексов защиты информации
20. Современные технические средства защиты информации.
21. Порядок проектирования системы защиты информации (СЗИ).
22. Оценки защищенности СЗИ. Критерии определения безопасности компьютерных систем
23. Программно-аппаратные средства, реализующие отдельные требования по обеспечению информационной безопасности.
24. Типовая структура комплексной системы защиты от несанкционированного доступа
25. Методы и средства ограничения доступа к компонентам вычислительных систем
26. Пример систем комплексной защиты информации СКЗИ (ViPNet, КриптоПро, Верба)
27. Методы и средства хранения и управления ключевой информацией
28. Основы ОС и безопасность ОС. (Windows & Linux)
29. Основы сетевых протоколов и сетевая безопасность, стек протоколов TCP/IP, IPSec, SSL, TLS.
30. Классификация основных типов сетевых атак; основные характеристики различных типов межсетевых экранов, анализ защищенности
31. Принципы построения виртуальных частных сетей (VPN) + туннелирование, безопасность маршрутизаторов с использованием списков контроля доступа и возможностей по протоколированию событий
32. Защита программ от изучения, способы встраивания средств защиты в ПО
33. Основные уязвимости при написании кода, безопасный код, ООП в ИБ
34. DevSecOps, тестирование на безопасность
35. Использование виртуальных машин в сфере обеспечения информационной безопасности.
36. Безопасность виртуальных и облачных технологий
37. Основные уязвимости web-сайтов и web-сервисов, основы безопасной разработки вебсервисов, сайтов, распределенные атаки типа "отказ в обслуживании"
38. Биометрия, типы, обучение, ошибки разного рода
39. Кибербезопасность BigData
40. BigData и искусственный интеллект в сфере информационной безопасности
41. Аудит информационной безопасности и методы проведения аудита систем и ПО
42. Порядок лицензирования деятельности в КБ
43. Разработка политики и программы безопасности
44. Основные классы мер процедурного уровня ИБ
45. Построение "демилитаризованных зон" (DMZ) для корпоративной сети
46. Принципы действия и типовая структура систем обнаружения вторжений (IDS)
47. Принципы действия и типовая структура систем предотвращения вторжений (IPS)
48. Принципы действия и типовая структура систем предотвращения утечек информации (DLP)
49. Управление информационной безопасностью и управление событиями безопасности SIEM
50. Принципы действия и типовая структура песочниц (sandbox) и ловушек (honeypots)
51. Идентификация и аутентификация, управление доступом
52. Протоколирование и аудит, шифрование, контроль целостности
53. Планы бесперебойной работы, реализация бесперебойного электропитания и резервного копирования данных
54. Сервисы безопасности. Архитектурная безопасность, классификация сервисов
55. Построение системы защищенной обработки конфиденциальных документов

Критерии оценивания

Оценка отлично (10) выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично (9) выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично (8) выставляется студенту, показавшему систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.

Оценка хорошо (7) выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.

Оценка хорошо (6) выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

Оценка хорошо (5) выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.

Оценка удовлетворительно (4) выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.

Оценка удовлетворительно (3) выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации.

Оценка неудовлетворительно (2) выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.

Оценка неудовлетворительно (1) выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

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

Дифференцированный зачёт проводится путем организации специального опроса, проводимого в устной и (или) письменной форме.

При проведении дифференцированного зачёта обучающемуся предоставляется 30 минут на подготовку. Опрос обучающегося по билету не должен превышать одного астрономического часа.

Во время проведения дифференцированного зачёта обучающиеся могут пользоваться программой дисциплины, а также справочной литературой.