Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ И ПРИЛОЖЕНИЙ

Блок:	**Блок 4 «Факультативы»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б4.Ч.07**
Трудоемкость в зачетных единицах:	**8 семестр - 2;**
Часов (всего) по учебному плану:	**72 часа**
Лекции	**8 семестр - 14 часов;**
Практические занятия	**8 семестр - 14 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**8 семестр - 43,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Коллоквиум**	
Промежуточная аттестация:	
Зачет	**8 семестр - 0,3 часа;**

Москва 2024

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: формирование системы понятий, знаний, умений и навыков в области деятельности, связанной с защитой информации при эксплуатации и обслуживании мобильных систем и приложений.

Задачи дисциплины

- изучение актуальных угроз и уязвимостей мобильных систем и способов защиты данных в них;
- администрирование систем и средств обеспечения информационной безопасности мобильных систем.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ПК-2 Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-3.З$_{ПК-2}$ Администрирует средства защиты информации прикладного и системного программного обеспечения	знать: - основы функционирования мобильных систем, возможные угрозы информационной безопасности и уязвимости специального и прикладного программного обеспечения при их эксплуатации злоумышленниками. уметь: - формулировать политику информационной безопасности для мобильных систем; - администрировать системное и программное обеспечение мобильных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Безопасность компьютерных систем (продвинутый уровень) (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Проблемы обеспечения безопасности мобильных устройств и приложений	27.7	8	6	-	6	-	-	-	-	-	15.7	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Проблемы обеспечения безопасности мобильных устройств и приложений" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Проблемы обеспечения безопасности мобильных устройств и приложений" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Проблемы обеспечения безопасности мобильных устройств и приложений" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу
1.1	Тема 1. Мобильные платформы. Защита информации	9.7		2	-	2	-	-	-	-	-	5.7	-	
1.2	Тема 2. Мобильные ОС Windows Mobile/ Windows Phone и ОС Android. Обзор актуальных угроз и средств защиты информации	9		2	-	2	-	-	-	-	-	5	-	
1.3	Тема 3. Классификация угроз безопасности информации и методы оценки безопасности мобильных систем и устройств	9		2	-	2	-	-	-	-	-	5	-	

														"Проблемы обеспечения безопасности мобильных устройств и приложений" ***Изучение материалов литературных источников:*** [3], 123-176 [4], 1-46 [5], 1-50
2	Обеспечение безопасности информации мобильных устройств и приложений	44		8	-	8	-	-	-	-	-	28	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Обеспечение безопасности информации мобильных устройств и приложений" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Обеспечение безопасности информации мобильных устройств и приложений" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Обеспечение безопасности информации мобильных устройств и приложений"
2.1	Тема 4. Защита мобильных устройств. Принципы обеспечения безопасности мобильных систем.	9		2	-	2	-	-	-	-	-	5	-	
2.2	Тема 5. Решение типовых проблем защиты мобильных устройств и приложений	17		2	-	2	-	-	-	-	-	13	-	
2.3	Тема 6. Защита от перехвата трафика в мобильных системах	9		2	-	2	-	-	-	-	-	5	-	
2.4	Тема 7. Мобильные веб-браузеры. Уязвимости. Средства защиты	9		2	-	2	-	-	-	-	-	5	-	

														подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Обеспечение безопасности информации мобильных устройств и приложений" ***<u>Изучение материалов литературных источников:</u>*** [1], 1-200 [2], 234-267
	Зачет	0.3		-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	**72.0**		**14**	**-**	**14**	**-**	**-**	**-**	**-**	**0.3**	**43.7**	**-**	
	Итого за семестр	**72.0**		**14**	**-**	**14**	**-**		**-**		**0.3**	**43.7**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Проблемы обеспечения безопасности мобильных устройств и приложений

1.1. Тема 1. Мобильные платформы. Защита информации

Место и роль мобильных устройств и приложений в управлении бизнес-процессами. Архитектура мобильных устройств. Причины обострения проблемы обеспечения информационной безопасности мобильных систем.

1.2. Тема 2. Мобильные ОС Windows Mobile/ Windows Phone и ОС Android. Обзор актуальных угроз и средств защиты информации

Мобильные ОС Windows Mobile/ Windows Phone и ОС Android: Возможности. Закрытые и открытые архитектуры, средства взаимодействия. Интерфейс.. Инструменты безопасности. Средства синхронизации. Уязвимости. Виды и примеры вредоносного ПО.. Антивирусные средства. Возможности шифрования данных. Политики безопасности.

1.3. Тема 3. Классификация угроз безопасности информации и методы оценки безопасности мобильных систем и устройств

Актуальность проблемы обеспечения безопасности мобильных устройств и приложений. Субъекты информационных отношений и их безопасность. Угрозы безопасности мобильных устройств и приложений. Модели угроз безопасности информации. Уязвимость основных структурно-функциональных элементов мобильных устройств и приложений.

2. Обеспечение безопасности информации мобильных устройств и приложений

2.1. Тема 4. Защита мобильных устройств. Принципы обеспечения безопасности мобильных систем.

Виды мер противодействия угрозам безопасности.. Принципы построения системы обеспечения безопасности информации в мобильных системах. Достоинства и недостатки различных видов мер защиты.

2.2. Тема 5. Решение типовых проблем защиты мобильных устройств и приложений

Стратегия обеспечения безопасности конфиденциальной информации в мобильных устройствах на основе внедрения систем MDM (Mobile Device Management). Защита мобильных устройств в корпоративной среде с использованием Trend Micro Mobile Security.

2.3. Тема 6. Защита от перехвата трафика в мобильных системах

Методы защиты сетевого трафика. Защита внутреннего трафика в локальной сети. Протоколы SSL/TLS. VPN соединение.

2.4. Тема 7. Мобильные веб-браузеры. Уязвимости. Средства защиты

Мобильные веб-браузеры. Сравнительный обзор. Уязвимости. Средства защиты.. Разновидность атак на веб-приложения. Выявление паттернов.

3.3. Темы практических занятий

1. 5. Защита мобильных устройств в случае кражи, утечки данных мобильных устройств, от вредоносных программ, от фишинга и телефонного спама.;
2. 2. Мобильная ОС Windows Mobile/ Windows Phone. Уязвимости. Виды и примеры вредоносного ПО;
3. 1. Архитектура и функционал мобильных устройств;
4. 3. Оценка вероятности угроз от мобильных устройств по отдельным категориям:

потеря или кража мобильного устройства; перехват данных, которые передаются по сетям Wi-Fi или 3G; захват данных через соединения Bluetooth; мобильные вирусы (включая вирусы электронной почты).;
5. 4. Политики безопасного использования мобильных устройств в различных областях.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Проблемы обеспечения безопасности мобильных устройств и приложений"
2. Обсуждение материалов по кейсам раздела "Обеспечение безопасности информации мобильных устройств и приложений"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Проблемы обеспечения безопасности мобильных устройств и приложений"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Обеспечение безопасности информации мобильных устройств и приложений"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)		Оценочное средство (тип и наименование)
		1	2	
Знать:				
основы функционирования мобильных систем, возможные угрозы информационной безопасности и уязвимости специального и прикладного программного обеспечения при их эксплуатации злоумышленниками	ПК-3.3$_{ПК-2}$	+		Коллоквиум/Информационная безопасность мобильных систем
Уметь:				
администрировать системное и программное обеспечение мобильных систем	ПК-3.3$_{ПК-2}$		+	Коллоквиум/Защита информации в мобильных системах Коллоквиум/Обеспечения безопасности конфиденциальной информации в мобильных устройствах
формулировать политику информационной безопасности для мобильных систем	ПК-3.3$_{ПК-2}$	+	+	Коллоквиум/Проблемы обеспечения безопасности мобильных устройств и приложений

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

8 семестр

Форма реализации: Устная форма

1. Защита информации в мобильных системах (Коллоквиум)
2. Информационная безопасность мобильных систем (Коллоквиум)
3. Обеспечения безопасности конфиденциальной информации в мобильных устройствах (Коллоквиум)
4. Проблемы обеспечения безопасности мобильных устройств и приложений (Коллоквиум)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет (Семестр №8)

В диплом выставляется оценка за 8 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие для среднего профессионального образования по группе специальностей 09.00.00 "Информатика и вычислительная техника" / В. Ф. Шаньгин. – М. : Форум : ИНФРА-М, 2018. – 415 с. – (Среднее профессиональное образование). – ISBN 978-5-8199-0754-2.;
2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие для вузов по направлению 09.03.01 "Информатика и вычислительная техника" / В. Ф. Шаньгин. – Москва : Форум : ИНФРА-М, 2020. – 592 с. – (Высшее образование. Бакалавриат). – ISBN 978-5-8199-0730-6.;
3. Олифер, В. Г. Основы компьютерных сетей : учебное пособие / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2014. – 352 с. – (Учебное пособие). – ISBN 978-5-496-00924-9.;
4. Олифер В. Г., Олифер Н. А.- "Основы сетей передачи данных", (2-е изд.), Издательство: "ИНТУИТ", Москва, 2016 - (219 с.)
https://e.lanbook.com/book/100346;
5. Девянин П. Н.- "Модели безопасности компьютерных систем. Управление доступом и информационными потоками", (2-е изд., испр. и доп.), Издательство: "Горячая линия-Телеком", Москва, 2017 - (338 с.)
https://e.lanbook.com/book/111049.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;

4. Видеоконференции (Майнд, Сберджаз, ВК и др).

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **Электронные ресурсы издательства Springer** - https://link.springer.com/
5. **База данных Web of Science** - http://webofscience.com/
6. **База данных Scopus** - http://www.scopus.com
7. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
8. **Журнал Science** - https://www.sciencemag.org/
9. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
10. **Портал открытых данных Российской Федерации** - https://data.gov.ru
11. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
12. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
13. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru
14. **Федеральный портал "Российское образование"** - http://www.edu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер

Помещения для самостоятельной работы	НТБ-303, Лекционная аудитория	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Безопасность мобильных устройств и приложений

(название дисциплины)

8 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Информационная безопасность мобильных систем (Коллоквиум)
КМ-2 Проблемы обеспечения безопасности мобильных устройств и приложений (Коллоквиум)
КМ-3 Обеспечения безопасности конфиденциальной информации в мобильных устройствах (Коллоквиум)
КМ-4 Защита информации в мобильных системах (Коллоквиум)

Вид промежуточной аттестации – Зачет.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Проблемы обеспечения безопасности мобильных устройств и приложений					
1.1	Тема 1. Мобильные платформы. Защита информации		+			
1.2	Тема 2. Мобильные ОС Windows Mobile/ Windows Phone и ОС Android. Обзор актуальных угроз и средств защиты информации		+			
1.3	Тема 3. Классификация угроз безопасности информации и методы оценки безопасности мобильных систем и устройств			+		
2	Обеспечение безопасности информации мобильных устройств и приложений					
2.1	Тема 4. Защита мобильных устройств. Принципы обеспечения безопасности мобильных систем.			+		
2.2	Тема 5. Решение типовых проблем защиты мобильных устройств и приложений				+	+
2.3	Тема 6. Защита от перехвата трафика в мобильных системах				+	+
2.4	Тема 7. Мобильные веб-браузеры. Уязвимости. Средства защиты				+	+
		Вес КМ, %:	20	20	30	30