МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы бакалавриата
по направлению подготовки
09.03.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): IT-сервисы и технологии обработки данных на транспорте

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Цель освоение дисциплины - формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи освоения дисциплины – научить студентов:

- понимать сущность информационной безопасности;

понимать принципы организации защиты информации на предприятиях;

выявлять основные виды угроз информационной безопасности;

Применять программно-аппаратные средства для обеспечения информационной безопасности

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ПК-3 - Способен осуществлять разработку требований и проектирование программного обеспечения;

ПК-8 - Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации;

ПК-9 - Способен обеспечивать информационную безопасность на уровне БД.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

основные понятия и принципы информационной безопасности,

основные шаблоны и параметры безопасности компьютерных систем,

виды и тип угроз информационной безопасности

Уметь:

Осуществлять аудит применяемого пользователями ПО с помощью политики управления приложениями AppLocker в Windows 10

Работать с с системой обнаружения атак Snort и сетевым анализатором Wireshark для выявления и анализа сетевых атак

Настраивать основные шаблоны и параметры безопасности компьютерных систем

Создавать и анализировать личные базы данных параметров безопасности в оснастке Security Configuration and Analysis 5

Владеть:

– навыком анализа сетевых ресурсов с использованием утилиты nmap,

– навыками настройки и применения политик безопасности в операционных системах Windows?

– навыками реагирования на сетевые атаки

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №6
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 44 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Тема 1. Обзор основных концепций корпоративной информационной безопасности Рассматриваемые вопросы: - Ключевые понятия, термины и определения - Ландшафт киберугроз - Домены результативной кибербезопасности
2	Тема 2. Криптографические средства и методы защиты информации Рассматриваемые вопросы: - Исторические шифры и методы их криптоанализа - Принципы Кергофса - Хеш-функции: алгоритмы и применение - Стандарты и алгоритмы симметричного шифрования - Алгоритм Диффи-Хелмана - Криптосистема RSA - Инфраструктура открытых ключей - Протокол SSL/TLS
3	Тема 3. Управление доступом Рассматриваемые вопросы: - Идентификация, аутентификация, авторизация, аудит - Пароль как фактор аутентификации. Энтропия паролей, парольная политика - Токены - Биометрические факторы аутентификации - Access Lists - Модели управления доступом: DAC, MAC, RBAC, ABAC - Identity Management (IdM)-решения - Privileged Access Management (PAM)-решения - Концепция Single Sign On (SSO)
4	Тема 4. Безопасность компьютерных сетей Рассматриваемые вопросы: - Физический, канальный и сетевой уровни модели OSI: MAC, Ethernet, ARP, IEEE 802.11, концентраторы, коммутаторы, маршрутизаторы, IPv4, адресация в локальных и глобальной сети, нотация CIDR, протоколы маршрутизации BGP, RIP. Атаки канального и сетевого уровней: MAC Authentication Bypass, LLDP reconnaissance, ARP Harvesting, ARP Cache Poisoning, CAM Table Owerflow Attack, SMB Relay, DHCP Spoofing. - Транспортный уровень: TCP, UDP, NAT/PAT, методы сканирования узлов/сетей, МСЭ, IDS/IPS, проектирование безопасной сетевой архитектуры. - Прикладной уровень: HTTP/HTTPS, DNS, архитектура web-приложений, OWASP Top 10.
5	Тема 5. Open Source Intelligence Рассматриваемые вопросы: - Сферы применения OSINT - OSINT framework - Уровни сети Интернет: Surface Web, Deep Web, Dark Web - Техники и практики OSINT: Google Dork Queries, DNS/WHOIS, Shodan/Censys Search/GreyNoise/ ZoomEye, httrack, web.archive, работа с метаданными файлов.
6	Тема 6. Основные компоненты и механизмы обеспечения безопасности инфраструктуры Windows Рассматриваемые вопросы: - Компоненты серверной инфраструктуры - Рабочие группы и домен - Структура Active Directory - Пользователи и Компьютеры

№ п/п	Тематика лекционных занятий / краткое содержание
	- AAA в Windows - Локальная аутентификация: winlogon.exe, lsass.exe, SAM - Протоколы сетевой аутентификации: LM, NTLM, Kerberos - Уязвимости AD: ZeroLogon, PathTheHash, SMBGhost, ProxyLogon, PrintNightmare
7	Тема 7. Компоненты безопасности ОС Linux Рассматриваемые вопросы: - Защита УЗ: SUDO, PAM, использование Root - IPTABLES - GnuPG и PGP - Настройка SSH - Журналирование - SELinux и AppArmor
8	Тема 8. Управление уязвимостями Рассматриваемые вопросы: - CVE, БДУ и другие идентификаторы уязвимостей - Критичность по CVSS: базовые, временные и контекстные метрики - Процесс управления уязвимостями: роли, этапы, методология, экспертиза, технология.
9	Тема 9. Мониторинг и анализ событий информационной безопасности (ИБ), реагирование на инциденты ИБ Рассматриваемые вопросы: - Теория анализа логов - Журналы событий Windows. Sysmon - Основы анализа трафика: Wireshark, Snort - SIEM - Cyber Kill Chain, Pyramid of Pain - Матрица MITRE ATT&CK
10	Тема 10. Отечественное законодательство в сфере информационной безопасности Рассматриваемые вопросы: - Стратегические документы: Доктрина информационной безопасности РФ, Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 гг., Стратегия национальной безопасности РФ - Системообразующие документы: ГК РФ, 149-ФЗ, 152-ФЗ, Перечень сведений конфиденциального характера - Государственные регуляторы в сфере ИБ: ФСТЭК России, ФСБ России, Минцифры, Роскомнадзор, Банк России - Отдельные направления регулирования: Государственные и муниципальные информационные системы, криптография и электронная подпись, государственная тайна, коммерческая тайна, банковская тайна, Защита связи, ПДн, ГосСОПКА, Критическая информационная инфраструктура, Предприятия транспортной сферы как субъекты КИИ.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Тема 1. Основы криптографии Рассматриваемые вопросы: - Разработка скрипта на языке Python для формирования различных хеш-функций из произвольных строковых данных

№ п/п	Тематика практических занятий/краткое содержание
	- Разработка скрипта на языке Python, реализующего функционал подбора по словарю исходных значений из списка хеш-функций - Изучение функционала утилит hashcat и John The ripper
2	Тема 2. Управление доступом Рассматриваемые вопросы: - ACL для файлов в Linux. CHMOD калькулятор. - Настройка локальных и доменных УЗ в Windows. Управление группами.
3	Тема 3. Безопасность компьютерных сетей. Часть первая. Рассматриваемые вопросы: - Практика использования wireshark: анализируем различные виды трафика (ARP, DNS, icmp, HTTP), поиск флагов.
4	Тема 4. Безопасность компьютерных сетей. Часть вторая. Рассматриваемые вопросы: - Практика использования nmap: инвентаризационное сканирование, определение открытых портов и сетевых служб, обнаружение уязвимостей, уклонение от обнаружения.
5	Тема 5. Безопасность компьютерных сетей. Часть третья Рассматриваемые вопросы: - Настройка iptables по заданным политикам.
6	Тема 6. Безопасность компьютерных сетей. Часть четвертая Рассматриваемые вопросы: - Эксплуатация веб-уязвимостей в BeeWAPP: Injections (HTML, XML, SQL), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Shellshock vulnerability (CGI), Heartbleed bug (OpenSSL)
7	Тема 7. OSINT Рассматриваемые вопросы: - Практика Google Dorks и exif.tools: найти ФИО и должность сотрудника, опубликовавшего последний документ на сайте. - Анализ версии сайта МИИТ в 2003 году. Поиск заданной информации. - Практика использования shodan: анализ доменов https://www.miit.ru/ и https://wish.rut.digital.
8	Тема 8. Безопасность Windows и AD Рассматриваемые вопросы: - Решение «blue room» на tryhackme (https://tryhackme.com/r/room/blue): определение подверженности целевого хоста к уязвимости ms17-010 (эксплойт eternal blue) - Получение первоначального доступа - Эскалация с использованием meterpreter - Нахождение флагов в целевой системе
9	Тема 9. Безопасность Linux Рассматриваемые вопросы: - Решение «LinuxPrivEsc room» на tryhackme (https://tryhackme.com/r/room/linuxprivesc): Эксплуатация ошибок в настройках прав доступа к файлам /etc/shadow, /etc/passwd - Повышение привилегий с использованием исполняемых через SUDO файлов - Эксплуатация неправильных настроек /etc/crontab - Внедрение в общий объект исполняемых файлов SUID/SGID - Кража паролей или ключей из файлов конфигураций/журналов - Эксплуатация уязвимостей ядра
10	Тема 10. Мониторинг и анализ событий ИБ Рассматриваемые вопросы: - Практика поиска, агрегации, фильтрации и визуализации машинных данных с использованием языка SPL в Splunk.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с учебной литературой
2	Подготовка к промежуточной аттестации.
3	Подготовка к текущему контролю.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2	https://e.lanbook.com/book/132242
2	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9	https://e.lanbook.com/book/165837

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

https://habr.com/ru - база знаний в виде статей, обзоров

https://journal.tinkoff.ru/short/ai-for-all/ - база данных нейронных сетей

https://vc.ru/services/916617-luchshie-neyroseti-bolshaya-podborka-iz-top-200-ii-generatorov-po-kategoriyam - база данных нейронных сетей

https://github.com/abalmumcu/bert-rest-api - профессиональная платформа для командой работы над проектов (нейронная сеть bert)

http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ

https://proglib.io/p/raspoznavanie-obektov-s-pomoshchyu-yolo-v3-na-tensorflow-2-0-2020-11-08 - профессиональная библиотека программистов

https://yandex.cloud/ru/blog/posts/2022/12/andrey-berger-and-yandex-cloud?utm_referrer=https%3A%2F%2Fyandex.ru%2F – библиотека профессиональных статей разработчиков Яндекс

https://yandex.cloud/ru/blog - библиотека профессиональных статей разработчиков Яндекс

https://tproger.ru/translations/opencv-python-guide - библиотека основных команд OpenCV

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

MS Office (Excel, Word)
Браузер Chrome
Текстовый редактор (Notepad++)
Система виртуализация HYPER-V или VMware Workstation
Wireshark
Snort
nmap

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

Компьютер преподавателя
Компьютеры студентов
Лазерный принтер
Проектор
Экран для проектора
Маркерная доска

9. Форма промежуточной аттестации:

Экзамен в 6 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, к.н. Академии "Высшая инженерная школа" Б.В. Игольников

Согласовано:

Заместитель директора академии Д.В. Паринов

Председатель учебно-методической комиссии Д.В. Паринов