

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
09.03.02 Информационные системы и технологии,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита данных

Направление подготовки: 09.03.02 Информационные системы и технологии

Направленность (профиль): Технологии искусственного интеллекта в транспортных системах

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде
электронного документа выгружена из единой
корпоративной информационной системы управления
университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 5665
Подписал: заведующий кафедрой Нутович Вероника
Евгеньевна
Дата: 01.09.2024

1. Общие сведения о дисциплине (модуле).

Основными целями дисциплины являются:

- формирование четкого понимания взаимосвязанности понятий информация и данные, безопасность информации, информационная безопасность, защита информации и защита данных;
- углубление знаний, формирование и развитие умений и навыков, направленных на обеспечение «цифровой гигиены» при решении задач управления транспортной логистикой на основе искусственного интеллекта.

Основными задачами дисциплины являются:

- ознакомление с теоретическими основами и средствами технической и криптографической защиты информации (данных);
- ознакомление с методологией безопасной разработки программного обеспечения по требованиям безопасности информации (данных), реагирования на признаки вредоносного кода и недекларированных возможностей;
- ознакомление с нормативной правовой базой обеспечения безопасности информации (данных), структурой и задачами государственной системы защиты информации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-6 - Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий.;

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

Знать:

- разновидности и классы средств защиты информации (данных) и требования по их применению;
- методы алгоритмизации и языки программирования, пригодные для практического применения в области информационных систем и технологий.

Уметь:

- принимать превентивные меры, направленные на нераспространение вредоносных программ и воспрепятствование использованию недекларированных возможностей в системах хранения, обработки и передачи данных, используемых при управлении транспортной логистикой на основе искусственного интеллекта;
- применять методы и средства анализа функциональных требований к программному обеспечению.

Владеть:

- применять порядок реагирования по признакам возникновения угроз безопасности информации (данных) в информационных системах и технологиях, используемых при управлении транспортной логистикой на основе искусственного интеллекта;
- навыками анализа функциональных требований к программному обеспечению.

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 №4 |
| Контактная работа при проведении учебных занятий (всего): | 48 | 48 |
| В том числе: | | |
| Занятия лекционного типа | 16 | 16 |
| 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 60 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 | <p>Защита данных – введение в понятийный аппарат</p> <p>Рассматриваемые вопросы:</p> <p>Информация и данные, защищаемая информация (данные), безопасность информации (данных), информационная безопасность, защита информации (данных). Государственная система защиты информации (данных)</p> |
| 2 | <p>Цифровая гигиена информационного общества и цифровой экономики</p> <p>Рассматриваемые вопросы:</p> <p>Понятие «цифровая гигиена», ее роль в обеспечении безопасности информации (данных) и противодействии социальной инженерии</p> |
| 3 | <p>Безопасность программного обеспечения</p> <p>Рассматриваемые вопросы:</p> <p>Методология и средства безопасной разработки, развертывания, эксплуатации (включая техническую поддержку) и вывода из эксплуатации программного обеспечения</p> |
| 4 | <p>Техническая защита информации (данных)</p> <p>Рассматриваемые вопросы:</p> <p>Объекты информатизации. Методология и средства технической защиты информации</p> |
| 5 | <p>Введение в техническую защиту информации (данных)</p> <p>Рассматриваемые вопросы:</p> <p>Понятийный аппарат о технической защите информации (данных), регулирование деятельности по технической защите информации, нормативные правовые акты по технической защите информации, модели нарушителя и угроз</p> |
| 6 | <p>Защита информации (данных) от несанкционированного доступа</p> <p>Рассматриваемые вопросы:</p> <p>Объекты информатизации. Способы и средства технической защиты информации (данных) от несанкционированного доступа</p> |
| 7 | <p>Защита информации (данных) от утечки по побочным каналам</p> <p>Рассматриваемые вопросы:</p> <p>Побочные каналы утечки информации (данных). Способы и средства защиты информации от утечки по каналам электромагнитных излучений и наводок.</p> |
| 8 | <p>Криптографическая защита информации (данных)</p> <p>Рассматриваемые вопросы:</p> <p>Методология и средства криптографической защиты информации</p> |
| 9 | <p>Введение в криптографическую защиту информации (данных)</p> <p>Рассматриваемые вопросы:</p> |

| № п/п | Тематика лекционных занятий / краткое содержание |
|----------|--|
| | Основы криптологии. Криптография и криptoанализ. Многообразие средств криптографической защиты информации. |
| 10 | Симметричные криптосистемы Рассматриваемые вопросы: Симметричные криптографические системы. Простейшие шифры. Реализация симметричных криптосистем. |
| 11 | Ассиметричные криптосистемы Рассматриваемые вопросы: Асимметричные криптографические системы. Алгоритм Диффи-Хэллмана. Шифр RSA. Реализация асимметричных криптосистем. |
| 12 | Электронная (цифровая) подпись Рассматриваемые вопросы: Электронная подпись и удостоверяющие центры. Виды электронной подписи, способы и средства ее формирования. Инфраструктура открытых ключей. |

4.2. Занятия семинарского типа.

Практические занятия

| № п/п | Тематика практических занятий/краткое содержание |
|----------|--|
| 1 | Защита данных – понятийный аппарат В результате выполнения практического задания студент ознакомиться с нормативными актами, определяющими понятия: информация и данные, защищаемая информация (данные), безопасность информации (данных), информационная безопасность, защита информации (данных), - а также состав и задачи Государственной системы защиты информации (данных) |
| 2 | Цифровая гигиена информационного общества и цифровой экономики В результате выполнения практического задания студент ознакомиться с примерами атак на информационные системы и объекты информатизации, вызванные нарушением правил «цифровой гигиены» |
| 3 | Безопасность программного обеспечения В результате выполнения практического задания студент ознакомиться с основными способами и типовыми безопасной разработки, развертывания, эксплуатации (включая техническую поддержку) и вывода из эксплуатации программного обеспечения |
| 4 | Введение в техническую защиту информации (данных) В результате выполнения практического задания студент ознакомиться с нормативными актами по технической защите информации, примерами моделей нарушителей и угроз, работа с Банком данных угроз безопасности информации ФСТЭК России |
| 5 | Защита информации (данных) от несанкционированного доступа В результате выполнения практического задания студент ознакомиться с нормативными правовыми актами по защите объектов информатизации и технической защите информации (данных) от несанкционированного доступа. Освоение простейших возможностей операционных систем средств вычислительной техники по управлению правами пользователей по доступу к информации (данным). |
| 6 | Защита информации (данных) от утечки по побочным каналам В результате выполнения практического задания студент ознакомиться с возможностями съема информации (данных) по каналам электромагнитных излучений и наводок. |
| 7 | Введение в криптографическую защиту информации (данных) В результате выполнения практического задания студент ознакомиться с нормативными актами по |

| № п/п | Тематика практических занятий/краткое содержание |
|----------|--|
| | криптографической защите информации, формирование перечня видов средств, относящихся к криптографическим. |
| 8 | Симметричные криптосистемы В результате выполнения практического задания студент разработает простейшей шифр замены средствами электронной таблицы (имитация шифратора). |
| 9 | Ассиметричные криптосистемы В результате выполнения практического задания студент разработает реализации алгоритма Диффи-Хэллмана средствами электронной таблицы (имитация генератора ключей). |
| 10 | Электронная (цифровая) подпись В результате выполнения практического задания студент исследует браузер на предмет применяемых средств электронной подписи. |

4.3. Самостоятельная работа обучающихся.

| № п/п | Вид самостоятельной работы |
|----------|--|
| 1 | Работа с лекционным материалом. |
| 2 | Работа с литературой. |
| 3 | Текущая подготовка к занятиям. |
| 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 | Андресс Джейсон Защита данных. От авторизации до аудита. — СПб.: Питер, 2021. — 272 с.: ил. — ISBN 978-5-4461-1733-8 Книга | https://www.rulit.me/data/programs/resources/pdf/Andress_Zashchita-dannyh-Ot-avtorizacii-do-audita-_RuLit_Me_676096.pdf?ysclid=l9wf7vxc91281596876 (дата обращения 23.09.22) |
| 2 | Коллинз Майкл. Защита сетей. Подход на основе анализа данных / пер. с анг. А.В. Добровольская. - Москва : ДМК Пресс, 2020. - 308 с. - ISBN | https://elibrary.ru/download/elibrary_22231941_55109536.pdf (дата обращения 23.09.2022) |

| | | |
|---|--|--|
| | 978-5-97060-649-0 Книга | |
| 3 | Михалевич И.Ф. Требования, принципы, практика создания отечественных аппаратно- программных платформ для автоматизированных систем в защищенном исполнении критической информационной инфраструктуры Российской Федерации // Интеллектуальные системы. Теория и приложения. 2018. Т. 22. № 4. С. 11-30 Статья из сборника (однотомник) | http://intsysjournal.org/pdfs/22-4.pdf (дата обращения 23.09.2022) |
| 4 | Калашников А.О., Михалевич И.Ф. Анализ систем классификации зашитенности автоматизированных и информационных систем значимых объектов критической информационной инфраструктуры Российской Федерации // Информация и безопасность. 2018. Т. 21, вып. 1. С. 28-37. Статья из сборника (однотомник) | https://elibrary.ru/download/elibrary_36435930_99740121.pdf (дата обращения 23.09.2022) |
| 5 | Михалевич И.Ф. Методы обеспечения безопасности программного обеспечения сложных | https://elibrary.ru/download/elibrary_41727545_45140817.pdf (дата обращения 23.09.2022) |

| | | |
|---|---|--|
| | информационно-управляющих систем // В сборнике: Управление развитием крупномасштабных систем (MLSD'2019). Материалы двенадцатой международной конференции. Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. 2019. С. 868-877 Статья из сборника (однотомник) | |
| 6 | Михалевич И.Ф. Цифровая гигиена информационного общества: влияние пандемии COVID-19 // REDS: Телекоммуникационные устройства и системы. 2022. Т.12. №3. С. 10-17 Статья из сборника (однотомник) | http://media-publisher.ru/wp-content/uploads/REDS-3-2022.pdf (дата обращения 23.09.2022) |
| 7 | Михалевич И.Ф. Кооперативные интеллектуальные транспортные системы: тенденции кибербезопасности // В сборнике: Интеллектуальные транспортные системы. Материалы Международной научно-практической конференции. Москва, 2022. С. 235-242 Статья из сборника (однотомник) | https://elibrary.ru/download/elibrary_48449757_33168465.pdf (дата обращения 23.09.2022) |
| 8 | Методы и средства комплексной защиты информации в | https://www.iprbookshop.ru/101925.html (дата обращения 05.10.2022) |

| | | |
|----|---|--|
| | технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 224 с. — ISBN 978-5-9515-0429-6. Учебное пособие | |
| 9 | Коржик, В. И. Основы криптографии : учебное пособие / В. И. Коржик, В. А. Яковлев. — Санкт-Петербург : Интермедия, 2017. — 312 с. — ISBN 978-5-89160-097-3. Учебное пособие | https://www.iprbookshop.ru/66798.html (дата обращения 05.10.2022) |
| 10 | Михалевич И.Ф, Проблемы создания доверенной среды функционирования автоматизированных систем управления в защищенном исполнении // XII Всероссийское совещание по проблемам управления ВСПУ-2014, Москва 16-19 июня 2014 г., ИПУ РАН, с. 9201-9207. Книга | https://elibrary.ru/download/elibrary_22231941_95742471.pdf (дата обращения: 23.09.22) |
| 11 | Клименко И.С. Информационная безопасность и защита информации: модели и методы управления / И.С. Клименко. - Москва : Инфра-М, 2021. - 180 с. - ISBN 978-5-16-015149-6. Книга | https://ibooks.ru/bookshelf/378012/reading (дата обращения: 31.10.2022) |

| | | |
|----|--|---|
| 12 | Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - Москва : Горячая Линия—Телеком, 2018. - 586 с. - ISBN 978-5-9912-0424-8. Книга | https://ibooks.ru/bookshelf/354357/reading (дата обращения: 31.10.2022). |
|----|--|---|

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

- база данных угроз безопасности информации ФСТЭК России-
<https://bdu.fstec.ru/threat-section>
- база данных уязвимостей Open Web Application Security Project OWASP
- <https://owasp.org/www-project-top-ten/>
- электронная система и блог Лаборатории Касперского -
<https://www.kaspersky.ru/resource-center>
- база знаний Positive Technologies - ptsecurity.com
- электронно-библиотечная система «Лань» - <https://e.lanbook.com/>
- электронно-библиотечная система «IPRbooks» - <https://iprbookshop.ru/>

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

- операционная система (Астра Линукс, Windows, Ubuntu);
- текстовый редактор (Мой офис, Libre Office, Word);
- электронные таблицы (Мой офис, Libre Office, Excel).

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

Учебные аудитории для проведения лекционных занятий должны быть оснащены компьютерной техникой для преподавателя и набором демонстрационного оборудования.

Учебные аудитории для проведения семинарских занятий должны быть оснащены компьютерной техникой для преподавателя и студентов, а также набором демонстрационного оборудования.

9. Форма промежуточной аттестации:

Экзамен в 4 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, старший научный
сотрудник, к.н. кафедры
«Управление и защита
информации»

И.Ф. Михалевич

Согласовано:

Заведующий кафедрой ЦТУТП

В.Е. Нутович

Председатель учебно-методической
комиссии

Н.А. Андриянова