**МИНОБРНАУКИ РОССИИ**
**Ярославский государственный университет им. П.Г. Демидова**

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета

_____ Нестеров П.Н.

20 июня 2023 г.

**Рабочая программа дисциплины**

**Технологии обеспечения информационной безопасности**

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

## 1. Цели освоения дисциплины

Дисциплина «Технологии обеспечения информационной безопасности» имеет целью ознакомить обучающегося с угрозами безопасности информации, моделями нарушителей и современными технологиями обеспечения информационной безопасности.

Дисциплина обеспечивает приобретение основных знаний, умений и навыков в области обеспечения информационной безопасностью, способствует освоению принципов корректного применения современных средств и методов защиты информации.

В результате изучения дисциплины студент должен:

*знать:*

- терминологию в области защиты информации от несанкционированного доступа, несанкционированного и неправомерного воздействий;
- угрозы безопасности информации в автоматизированных системах;
- модели нарушителей;
- современные технологии защиты информации;
- требования нормативных документов ФСТЭК России по защите автоматизированных систем от несанкционированного доступа к информации;

*уметь:*

- осуществлять выбор функциональной структуры системы обеспечения безопасности информации, обрабатываемой в автоматизированных системах;
- обосновывать выбор технологий для обеспечения безопасности информации, обрабатываемой в автоматизированных системах;
- устанавливать, настраивать, тестировать и отлаживать программные и программно-аппаратные средства защиты информации;

*владеть:*

- анализа технологий и средств защиты информации от несанкционированного доступа.

## 2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к обязательной части образовательной программы.

Дисциплина «Технологии обеспечения информационной безопасности» является базовой для изучения большинства последующих дисциплин данной образовательной программы.

Полученные в курсе «Технологии обеспечения информационной безопасности» знания необходимы для изучения дисциплин «Управление информационной безопасностью», «Экономические вопросы обеспечения информационной безопасности», «Аудит информационной безопасности», «Защита программ и данных», «Защищенные информационные системы», «Аудит информационной безопасности», «Сложностная криптография», «Основы технологии блокчейн».

## 3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

| **Формируемая компетенция (код и формулировка)** | **Индикатор достижения компетенции (код и формулировка)** | **Перечень планируемых результатов обучения** |
|---|---|---|
| **Общепрофессиональные компетенции** | | |
| ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание | И-ОПК-1.2 Умеет классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности | Знает:<br>- терминологию в области защиты информации от несанкционированного доступа, несанкционированного и неправомерного воздействий;<br>- угрозы безопасности информации в автоматизированных системах;<br>- модели нарушителей;<br>- требования нормативных документов ФСТЭК России по защите автоматизированных систем от несанкционированного доступа к информации. |
| | И-ОПК-1.3 Умеет формулировать основные требования по защите конфиденциальной информации, в том числе персональных данных | Владеть навыками:<br>- обосновывать выбор технологий для обеспечения безопасности информации, обрабатываемой в автоматизированных системах. |
| ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности | И-ОПК-2.3 Знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации | Знает:<br>- современные технологии защиты информации. |
| | И-ОПК-2.4 Умеет настраивать основные средства защиты информации | Умеет:<br>- осуществлять выбор функциональной структуры системы обеспечения безопасности информации, обрабатываемой в автоматизированных системах;<br>- устанавливать, настраивать, тестировать и отлаживать программные и программно-аппаратные средства защиты информации. |

## 4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 акад. часов.

| № п/п | Темы (разделы) дисциплины, их содержание | Семестр | Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах) | | | | | | Формы текущего контроля успеваемости<br><br>Форма промежуточной аттестации (по семестрам) |
|---|---|---|---|---|---|---|---|---|---|
| | | | Контактная работа | | | | | | |
| | | | лекции | практические | лабораторные | консультации | аттестационные испытания | самостоятельная работа | |
| 1 | Классификация автоматизированных систем | 1 | 2 | 2 | | | | 2 | Задания для самостоятельной работы |
| 2 | Классификация угроз безопасности информации при обработке в автоматизированных системах (АС) | 1 | 4 | 4 | | | | 2 | Задания для самостоятельной работы |
| 3 | Модели угроз безопасности информации, обрабатываемой в АС. Классификация нарушителей | 1 | 4 | 4 | | | | 4 | Задания для самостоятельной работы |
| 4 | Классификация способов обеспечения безопасности информации, обрабатываемой в АС. | 1 | 4 | 4 | | | | 4 | Задания для самостоятельной работы |
| 5 | Современные технологии идентификации и аутентификации | 1 | 2 | 2 | 4 | | | 4 | Задания для самостоятельной работы |
| 6 | Современные технологии управления доступом к информации, обрабатываемой АС | 1 | 2 | 2 | 4 | | | 4 | Задания для самостоятельной работы |
| 7 | Современные технологии обеспечения целостности информации | 1 | 2 | 2 | 4 | | | 4 | Задания для самостоятельной работы |
| 8 | Современные технологии защиты информации и программного обеспечения от вредоносных программ | 1 | 2 | 2 | 4 | | | 4 | Задания для самостоятельной работы |
| 9 | Современные технологии регистрации и учета | 1 | 2 | 2 | 4 | | | 4 | Задания для самостоятельной работы |
| 10 | Современные технологии | 1 | 2 | 2 | 4 | | | 4 | Задания для |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | межсетевого экранирования | | | | | | | | самостоятельной работы |
| 11 | Методы и средства мониторинга событий ИБ | 1 | 2 | 2 | 8 | | | 8 | Задания для самостоятельной работы |
| 12 | Инциденты информационной безопасности | 1 | 4 | 4 | | | | 4 | Задания для самостоятельной работы |
| | | 1 | | | | | 0,5 | 33,5 | Экзамен |
| | **ИТОГО** | | **32** | **32** | **32** | | **0,5** | **81,5** | |

**Содержание дисциплины «Технологии обеспечения информационной безопасности»:**

Тема 1. Классификация автоматизированных систем.

Классификация информации по видам доступа. Документы, регламентирующие вопросы обработки конфиденциальной информации. Защита от НСД к информации. Классификация АС и требования по ЗИ. Требования и рекомендации по защите информации, обрабатываемой СВТ.

Тема 2. Классификация угроз безопасности информации при обработке в автоматизированных системах (АС).

Классификация угроз безопасности информации. Источники уязвимостей АС и их характеристика. Источники угроз безопасности информации. Общая характеристика: угроз непосредственного доступа в операционную среду АС; угроз безопасности, реализуемых с использованием протоколов межсетевого взаимодействия; угроз программно-математических воздействий; нетрадиционных информационных каналов и т.д. Методы реализации угроз безопасности информации.

Тема 3. Модели угроз безопасности информации, обрабатываемой в АС. Классификация нарушителей.

Методики определения актуальных угроз безопасности информации и уязвимостей АС. Типовые модели угроз безопасности информации, обрабатываемых в АС. Классификация и модели нарушителей. Модели безопасности информации.

Тема 4. Классификация способов обеспечения безопасности информации, обрабатываемой в АС.

Принципы построения системы обеспечения информационной безопасности (СОИБ). Требования к построению СОИБ. Классификация способов обеспечения информационной безопасности (управление доступом; регистрация и учет; обеспечение целостности; контроль отсутствия недекларированных возможностей; антивирусная защита; криптографическая защита информации; межсетевое экранирование и сегментирование сетей; анализ защищенности и обнаружение вторжений; предотвращение утечек и т. д.).

Тема 5. Современные технологии идентификации и аутентификации.

Аутентификация, авторизация и идентификация (определения). Технологии аутентификации: одноразовые пароли, многоразовые пароли, базы учетных записей, многофакторная аутентификация. Технологии идентификации и аутентификации пользователей по специальным устройствам. Технологии идентификации и аутентификации пользователей по биометрическим характеристикам человека. Технологии идентификации и аутентификации используемых компонентов обработки информации (аппаратных и программных средств).

Тема 6. Современные технологии управления доступом к информации, обрабатываемой АС.

Технологии управления доступом к АРМ и серверам. Технологии управления учетными записями. Технологии управления доступом к Web-ресурсам. Технологии однократной аутентификации пользователей. Технологии управления доступом к данным и к периферийным устройствам.

Тема 7. Современные технологии обеспечения целостности информации.

Основные требования к подсистеме обеспечения целостности информации. Подсистема резервного копирования: основные требования к подсистеме резервного копирования; типы резервного копирования; типы резервных носителей; хранение и использование резервных копий; архитектура подсистемы резервного копирования. Подсистема распределения обновлений: основные требования к подсистеме распределения обновлений; возможные варианты построения системы; архитектура подсистемы распределения обновлений. Восстановление программного обеспечения информации после сбоев и отказов оборудования и программно-математического воздействия.

Тема 8. Современные технологии защиты информации и программного обеспечения от вредоносных программ.

Основные к подсистеме антивирусной защиты. Методы защиты от вредоносных программ. Общая архитектура подсистемы антивирусной защиты. Выбор средств антивирусной защиты. Технологии контроля программного обеспечения на отсутствие недекларированных возможностей.

Тема 9. Современные технологии регистрации и учета.

Технологии предотвращения утечки конфиденциальной информации. Технологии регистрации субъектов доступа при входе/выходе в систему, запуске/завершении программ и процессов, доступе программных средств к файлам. Технологии регистрации выдачи печатных (графических) документов на «твердую» копию. Технологии регистрации доступа программных средств к аппаратным средствам. Защита информации от утечки - DLP-решения.

Тема 10. Современные технологии межсетевого экранирования.

Технологии межсетевого экранирования и сегментирования сети. Разновидности межсетевых экранов. Создание демилитаризованных зон. Технологии защищенного удаленного доступа к ресурсам ЛВС. Технологии контроля доступа пользователей к ресурсам сети Интернет. Технологии контентной фильтрации.

Тема 11. Методы и средства мониторинга событий ИБ.

Контроль и мониторинг событий ИБ. Обнаружение/предотвращение атак и нарушений политик безопасности (IDS/IPS): система предотвращения вторжений; классификация IPS: «сетевые» и «хостовые»; состав IPS. Аудит и анализ защищенности.

Тема 12. Инциденты информационной безопасности.

Нормативные документы по управлению инцидентами ИБ. Определение и перечень инцидентов ИБ. Уровень критичности инцидентов ИБ. Разделение функций управления ИБ. Основные принципы обработки инцидентов ИБ.

## 5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

**Вводная лекция** – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

**Академическая лекция** (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

**Лекция-беседа** или «диалог с аудиторией», является наиболее распространенной и сравнительно простой формой активного вовлечения студентов в учебный процесс. Эта лекция предполагает непосредственный контакт преподавателя с аудиторией. Преимущество лекции-беседы состоит в том, что она позволяет привлекать внимание студентов к наиболее важным вопросам темы, определять содержание и темп изложения учебного материала с учетом особенностей студентов.

**Проблемная лекция** – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала. Проблемная лекция начинается с вопросов, с постановки проблемы, которую в ходе изложения материала необходимо решить. В лекции сочетаются проблемные и информационные начала. При этом процесс познания студентов в сотрудничестве и диалоге с преподавателем приближается к поисковой, исследовательской деятельности. Содержание проблемы раскрывается путем организации поиска ее решения или суммирования и анализа традиционных и современных точек зрения.

**Практическое занятие** – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

**Лабораторная работа** – организация учебной работы с реальными материальными и информационными объектами.

**6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине**

В процессе осуществления образовательного процесса используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTex;
- Adobe Acrobat Reader;

при проведении практических занятий используется программное обеспечение:

- ПО "Dallas Lock 8.0-K";
- ПО "ViPNet Client 4.x (КС3)";
- ViPNet Administrator 4.5;
- Система защиты приложений от несанкционированного доступа Positive Technologies Application Firewal, конфигурация Education;
- MaxPatrol конфигурация Education;
- MaxPatrol Security Information and Event Management, конфигурация Education;
- XSpider, конфигурация Education;

при проведении практических занятий используется программно-аппаратное обеспечение:

- ПАК "Соболь" версии 4;
- СЗИ от НСД "Dallas Lock" (аппаратный);
- ViPNet Coordinator 4.5.

**7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)**

Для поиска учебной литературы библиотеки ЯрГУ используется автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php.

**8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины**

**а) основная литература**

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин - М.: ДМК Пресс, 2012. - 592 с.

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277 (дата обращения: 28.01.2022)

**б) дополнительная литература**

1. Мельников В. П. Информационная безопасность и защита информации: учеб. пособие для вузов. / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова; УМО по университет. политехн. образованию – 4-е изд., стереотип. – М: Академия, 2009. – 331 с.

2. Методика оценки угроз безопасности информации. Методический документ. Утвержден ФСТЭК России от 5 февраля 2021 г.

3. Меры защиты информации в государственных информационных системах, Методический документ. Утвержден ФСТЭК России от 11 февраля 2014 г.

4. Регламент включения информации об уязвимостях программного обеспечения ипрограммно-аппаратных средств банк данных угроз безопасности информации ФСТЭК России.

5. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Руководящий документ. Приказ председателя Гостехкомиссии России от 19 июня 2002 г. № 187.

6. Серия стандартов ИСО 27000 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности».

7. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019 (дата обращения: 28.01.2022)

**в) ресурсы сети «Интернет» (при необходимости)**

https://github.com/ – веб-сервис для размещения IT-проектов и их совместной разработки.

**9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине**

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения лабораторных работ, оснащенные средствами вычислительной техники, с установленным программным и программно-аппаратным обеспечением ПО "Dallas Lock 8.0-K"; ПО "ViPNet Client 4.x (КС3)"; ПАК "Соболь" версии 4; СЗИ от НСД "Dallas Lock" (аппаратный); ViPNet Administrator 4.5; 2 ViPNet Coordinator 4.5; Система защиты приложений от несанкционированного доступа Positive Technologies Application Firewal, конфигурация Education; MaxPatrol конфигурация Education; MaxPatrol Security Information and Event Management, конфигурация Education; XSpider, конфигурация Education;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;

– помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент кафедры КБиММОИ, канд. физ.-мат. наук Д.М. Мурин

**Приложение № 1 к рабочей программе дисциплины**
**«Технологии обеспечения информационной безопасности»**

**Фонд оценочных средств**
**для проведения текущего контроля успеваемости**
**и промежуточной аттестации студентов**
**по дисциплине**

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

**Практические работы(И-ОПК-1.2, И-ОПК-1.3)**

1. Выявление угроз безопасности информации.
2. Технологии управления доступом. Подготовка проектов технического задания и технического проекта.
3. Технологии обеспечения целостности информации.
4. Технологии антивирусной защиты. Подготовка проектов технического задания и технического проекта.
5. Технологии криптографической защиты информации. Подготовка проектов технического задания и технического проекта.
6. Технологии восстановления системного и прикладного программного обеспечения после сбоев и отказов оборудования и программно-математического воздействия.
7. Технологии межсетевого экранирования. Подготовка проектов технического задания и технического проекта.
8. Технологии систем обнаружения вторжений и анализа защищенности. Подготовка проектов технического задания и технического проекта.

**Лабораторные работы (И-ОПК-2.3, И-ОПК-2.4)**

1. Настройка Static Route.
2. Настройка Dinamic Route.
3. Настройка VLAN.
4. Настройка SSH.
5. Атака MAC-Flooding и методы противодействия ей.
6. Атака MAC-Spoofing и методы противодействия ей.
7. Атака ARP-Spoofing и методы противодействия ей.
8. Атака DHCP-spoofing и методы противодействия ей
9. Атака SSL – Split и методы противодействия ей.
10. Атака SSL – Strip и методы противодействия ей.
11. Атака подмена DNS и методы противодействия ей.

**Задания для самостоятельной работы**

Задания для самостоятельной работы состоят в самостоятельном повторении изученного материала и в доработке практических и лабораторных работ.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

**Список вопросов к экзамену:**

1. Классификация информации по видам доступа.
2. Документы, регламентирующие вопросы обработки конфиденциальной информации.
3. Классификация АС и требования по ЗИ.
4. Требования и рекомендации по защите информации, обрабатываемой СВТ.
5. Классификация угроз безопасности информации.
6. Источники уязвимостей АС и их характеристика. Источники угроз безопасности информации.
7. Общая характеристика: угроз непосредственного доступа в операционную среду АС; угроз безопасности, реализуемых с использованием протоколов межсетевого взаимодействия; угроз программно-математических воздействий; нетрадиционных информационных каналов и т.д.
8. Методы реализации угроз безопасности информации.
9. Методики определения актуальных угроз безопасности информации и уязвимостей АС.
10. Типовые модели угроз безопасности информации, обрабатываемых в АС.
11. Классификация и модели нарушителей. Модели безопасности информации.
12. Принципы построения системы обеспечения информационной безопасности (СОИБ).
13. Требования к построению СОИБ.
14. Классификация способов обеспечения информационной безопасности (управление доступом; регистрация и учет; обеспечение целостности; контроль отсутствия недекларированных возможностей; антивирусная защита; криптографическая защита информации; межсетевое экранирование и сегментирование сетей; анализ защищенности и обнаружение вторжений; предотвращение утечек и т. д.).
15. Аутентификация, авторизация и идентификация (определения).
16. Технологии аутентификации: одноразовые пароли, многоразовые пароли, базы учетных записей, многофакторная аутентификация.
17. Технологии идентификации и аутентификации пользователей по специальным устройствам.
18. Технологии идентификации и аутентификации пользователей по биометрическим характеристикам человека.
19. Технологии идентификации и аутентификации используемых компонентов обработки информации (аппаратных и программных средств).
20. Технологии управления доступом к АРМ и серверам.
21. Технологии управления учетными записями.
22. Технологии управления доступом к Web-ресурсам.
23. Технологии однократной аутентификации пользователей.
24. Технологии управления доступом к данным и к периферийным устройствам.
25. Основные требования к подсистеме обеспечения целостности информации.
26. Подсистема резервного копирования: основные требования к подсистеме резервного копирования; типы резервного копирования; типы резервных носителей; хранение и использование резервных копий; архитектура подсистемы резервного копирования.
27. Подсистема распределения обновлений: основные требования к подсистеме распределения обновлений; возможные варианты построения системы; архитектура подсистемы распределения обновлений.
28. Восстановление программного обеспечения информации после сбоев и отказов оборудования и программно-математического воздействия.
29. Основные к подсистеме антивирусной защиты.
30. Методы защиты от вредоносных программ. Общая архитектура подсистемы антивирусной защиты.

31. Выбор средств антивирусной защиты. Технологии контроля программного обеспечения на отсутствие недекларированных возможностей.
32. Технологии предотвращения утечки конфиденциальной информации.
33. Технологии регистрации субъектов доступа при входе/выходе в систему, запуске/завершении программ и процессов, доступе программных средств к файлам.
34. Технологии регистрации выдачи печатных (графических) документов на «твердую» копию.
35. Технологии регистрации доступа программных средств к аппаратным средствам.
36. Защита информации от утечки - DLP-решения.
37. Технологии межсетевого экранирования и сегментирования сети.
38. Разновидности межсетевых экранов.
39. Создание демилитаризованных зон.
40. Технологии защищенного удаленного доступа к ресурсам ЛВС.
41. Технологии контроля доступа пользователей к ресурсам сети Интернет.
42. Технологии контентной фильтрации.
43. Контроль и мониторинг событий ИБ.
44. Обнаружение/предотвращение атак и нарушений политик безопасности (IDS/IPS): система предотвращения вторжений; классификация IPS: «сетевые» и «хостовые»; состав IPS.
45. Нормативные документы по управлению инцидентами ИБ.
46. Определение и перечень инцидентов ИБ. Уровень критичности инцидентов ИБ.
47. Разделение функций управления ИБ.
48. Основные принципы обработки инцидентов ИБ.

**Правила выставления оценки на экзамене.**

В экзаменационный билет включаются два теоретических вопроса. На подготовку к ответу дается не менее 1 академического часа.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

**Оценка «Отлично»** выставляется студенту, который успешно сдал все лабораторные и практические работы и демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом защиты информации; умеет связывать теорию с практикой. Студент дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует терминологию.

**Оценка «Хорошо»** выставляется студенту, который успешно сдал все лабораторные и практические работы и ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

**Оценка «Удовлетворительно»** выставляется студенту, который успешно сдал все лабораторные и практические работы, возможно за исключением одной из них, и дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и

несущественные признаки и установить причинно-следственные связи. Ответы излагаются с использованием терминологии защиты информации, но при этом допускаются ошибки в определениях некоторых основных понятий, формулировках положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

**Оценка «Неудовлетворительно»** выставляется студенту, который не сдал более одной лабораторной или практической работы, и демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении сущности раскрываемых понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

**Приложение № 2 к рабочей программе дисциплины**
**«Технологии обеспечения информационной безопасности»**

## Методические указания для студентов по освоению дисциплины

Учебным планом на изучение дисциплины «Технологии обеспечения информационной безопасности» отводится один семестр, по завершении которого в качестве итогового контроля предусмотрен экзамен. В процессе изучения дисциплины проводятся практические и лабораторные работы, выполняются двенадцать домашних заданий.

Для успешного освоения дисциплины важно, чтобы обучающийся уделил особенное внимание выполнению практических и лабораторных работ. Теоретические основы, необходимые для выполнения этих работ, подробно разбираются на лекционных занятиях. Основная цель выполнения практических и лабораторных работ – дать обучающимся представление о применении технологий обеспечения информационной безопасности на практике. Для успешного выполнения практических и лабораторных работ необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала, чему способствуют регулярные задания для самостоятельной работы. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических и лабораторных занятиях и из учебной литературы.

В качестве заданий для самостоятельной работы дома обучающимся предлагается доработать задания практических и лабораторных работ, выполнение которых начинается в аудитории.

По итогам изучения дисциплины обучающиеся сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к экзамену предусмотрена групповая консультация.

Опыт преподавания дисциплины «Технологии обеспечения информационной безопасности» говорит о сложности ее самостоятельного изучения для обучающегося, несмотря на наличие достаточно качественных учебных пособий. Это связано с большим числом лабораторных работ, необходимых для приобретения навыков практического использования изучаемого материала. Поэтому посещение всех аудиторных занятий является настоятельно рекомендуемым.