

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение высшего образования  
"Казанский (Приволжский) федеральный университет"  
Институт физики



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Е.А. Турилова

17 февраля 2023 г.

*подписано электронно-цифровой подписью*

## Программа дисциплины

Теоретические основы компьютерной безопасности

Специальность: 10.05.03 - Информационная безопасность автоматизированных систем

Специализация: Безопасность открытых информационных систем

Квалификация выпускника: специалист по защите информации

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2023

## Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО
2. Место дисциплины (модуля) в структуре ОПОП ВО
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
  - 4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)
  - 4.2. Содержание дисциплины (модуля)
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
6. Фонд оценочных средств по дисциплине (модулю)
7. Перечень литературы, необходимой для освоения дисциплины (модуля)
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)
12. Средства адаптации преподавания дисциплины (модуля) к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья
13. Приложение №1. Фонд оценочных средств
14. Приложение №2. Перечень литературы, необходимой для освоения дисциплины (модуля)
15. Приложение №3. Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Программу дисциплины разработал(а)(и): доцент, к.н. (доцент) Насыров И.А. (Кафедра радиоэлектроники, Высшая школа киберфизических систем и прикладной электроники), Igor.Nasyrov@kpfu.ru

### 1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- методологические и технологические основы комплексного обеспечения безопасности АС,
- угрозы и методы нарушения безопасности АС,
- формальные модели, лежащие в основе систем защиты АС,
- стандарты по оценке защищенности АС и их теоретические основы,
- методы и средства реализации защищенных АС,
- методы и средства верификации и анализа надежности защищенных АС;

Должен уметь:

- проводить анализ АС с точки зрения обеспечения компьютерной безопасности,
- разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы,
- применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС,
- реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС;

Должен владеть:

навыками:

- работы с АС распределенных вычислений и обработки информации;
- работы с документацией АС,
- использования критериев оценки защищенности АС,
- построения формальных моделей систем защиты информации АС.

Должен демонстрировать способность и готовность:

- проводить анализ АС с точки зрения обеспечения компьютерной безопасности,
- разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы,
- применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС,
- реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС;

иметь навыки:

- работы с АС распределенных вычислений и обработки информации;
- работы с документацией АС,
- использования критериев оценки защищенности АС,

- построения формальных моделей систем защиты информации АС.

## 2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.О.30 Дисциплины (модули)" основной профессиональной образовательной программы 10.05.03 "Информационная безопасность автоматизированных систем (Безопасность открытых информационных систем)" и относится к обязательной части ОПОП ВО.

Осваивается на 3 курсе в 5 семестре.

## 3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) на 108 часа(ов).

Контактная работа - 54 часа(ов), в том числе лекции - 34 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 20 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 18 часа(ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 5 семестре.

## 4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

### 4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Се- местр	Виды и часы контактной работы, их трудоемкость (в часах)						Само- стоя- тель- ная ра- бота
			Лекции, всего	Лекции в эл. форме	Практи- ческие занятия, всего	Практи- ческие в эл. форме	Лабора- торные работы, всего	Лабора- торные в эл. форме	
1.	Тема 1. Структура теории компьютерной безопасности. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности.	5	4	0	0	0	0	0	2
2.	Тема 2. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы данных.	5	4	0	0	0	0	0	2
3.	Тема 3. Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.	5	4	0	0	0	0	0	2
4.	Тема 4. Методология построения систем защищенных АС. Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.	5	4	0	0	0	6	0	0

N	Разделы дисциплины / модуля	Се- местр	Виды и часы контактной работы, их трудоемкость (в часах)						Само- стоя- тель- ная ра- бота
			Лекции, всего	Лекции в эл. форме	Практи- ческие занятия, всего	Практи- ческие в эл. форме	Лабора- торные работы, всего	Лабора- торные в эл. форме	
5.	Тема 5. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.	5	4	0	0	0	4	0	4
6.	Тема 6. Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).	5	4	0	0	0	4	0	2
7.	Тема 7. Политика безопасности. Понятие политики безопасности Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.	5	4	0	0	0	2	0	2
8.	Тема 8. Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL).	5	4	0	0	0	0	0	2
9.	Тема 9. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.	5	2	0	0	0	0	0	2
10.	Тема 10. Защита информации от внутренних угроз. Защищаемый периметр информации. Предотвращение утечек (Data Loss Prevention, DLP) - технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек. Решения SearchInform.	5	0	0	0	0	4	0	0
	Итого		34	0	0	0	20	0	18

## 4.2 Содержание дисциплины (модуля)

**Тема 1. Структура теории компьютерной безопасности. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности.**

Структура теории компьютерной безопасности. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности.

---

**Тема 2. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы данных.**

Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы данных.

---

**Тема 3. Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.**

Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.

---

**Тема 4. Методология построения систем защищенных АС. Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.**

Методология построения систем защищенных АС. Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

---

**Тема 5. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.**

Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.

---

**Тема 6. Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).**

Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).

---

**Тема 7. Политика безопасности. Понятие политики безопасности Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.**

Политика безопасности. Понятие политики безопасности Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.

---

**Тема 8. Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL).**

Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL).

---

**Тема 9. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.**

Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.

---

**Тема 10. Защита информации от внутренних угроз. Защищаемый периметр информации. Предотвращение утечек (Data Loss Prevention, DLP) - технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек. Решения SearchInform.**

Установка и первоочередная настройка программного комплекса SearchInform.

Принципы использования программного комплекса SearchInform для мониторинга утечек конфиденциальной информации.

Настройка программного комплекса SearchInform для контроля содержимого экранов пользователей и поиска конфиденциальной информации без проведения синтаксического анализа.

Настройка программного комплекса SearchInform для поиска конфиденциальной информации на основе подобия текстовых фрагментов.

Формирование регулярных выражений и настройка системы перехвата передаваемой информации.

**5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)**

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства науки и высшего образования Российской Федерации от 6 апреля 2021 года №245)

Письмо Министерства образования Российской Федерации №14-55-99бин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

Ассиметричное шифрование - <https://habr.com/ru/articles/748226/>

Симметричное шифрование - <https://ubiklab.net/posts/symmetric-encryption/>

Теоретические основы компьютерной безопасности - <https://habr.com/ru/articles/682154/>

**6. Фонд оценочных средств по дисциплине (модулю)**

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

## 7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;

- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

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

Харбакор. Криптография - <http://habrahabr.ru/hub/crypto/>

Введение в криптографию - <http://algolist.manual.ru/defence/intro.php>

Глоссарий криптографических терминов - <http://www.enlight.ru/crypto/glossary/glossary.htm>

Информзащита - <http://itsecurity.ru/catalog/bt01>

Криптографический ликбез - <http://www.ssl.stu.neva.ru/psw/crypto.html>

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

Вид работ	Методические рекомендации
лекции	При изучении и проработке теоретического материала для студентов необходимо: - повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы; - при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в учебной программе литературные и интернет источники; - ответить на контрольные вопросы по темам и разделам дисциплины.
лабораторные работы	Лабораторные работы проводятся с целью углубления и закрепления знаний, полученных на лекциях и в процессе самостоятельной работы над учебной и научной литературой. При подготовке к лабораторной работе студентам необходимо: - изучить, повторить теоретический материал по заданной теме; - изучить материалы лабораторной работы по заданной теме, уделяя особое внимание расчетным формулам; - при выполнении расчетных заданий, изучить, повторить типовые задания, выполняемые в аудитории.
самостоятельная работа	Самостоятельная работа студентов включает подготовку к устному опросу. Для этого студент изучает лекции, основную и дополнительную литературу, публикации, информацию из Интернет-ресурсов. Эффективность подготовки студентов зависит от качества ознакомления с рекомендованной литературой. Для подготовки к устному опросу студенту необходимо ознакомиться с материалом, посвященным изучаемой теме в учебнике или другой рекомендованной литературе, записях с лекционного занятия. Развернутый ответ должен следовать определенной логике и последовательности изложения, состоять из многих предложений, содержать доводы и выводы. Критерии оценки: оценки студентов будут зависеть от полноты ответов на вопросы, уровня начитанности, наличия убедительных фактов и аргументов, логики изложения, языка и стиля, глубины анализа источников.



Вид работ	Методические рекомендации
экзамен	<p>Готовиться к экзамену необходимо последовательно, с учетом контрольных вопросов, разработанных преподавателем кафедры. Сначала следует определить место каждого контрольного вопроса в соответствующем разделе темы учебной программы, а затем внимательно прочитать и осмыслить рекомендованные научные работы, соответствующие разделы рекомендованных учебников. При этом полезно делать краткие выписки и заметки. Работу над темой можно считать завершенной, если вы сможете ответить на все контрольные вопросы и дать определение понятий по изучаемой теме.</p> <p>Для обеспечения полноты ответа на контрольные вопросы и лучшего запоминания теоретического материала рекомендуется составлять план ответа на контрольный вопрос. Это позволит сэкономить время для подготовки непосредственно перед экзаменом за счет обращения не к литературе, а к своим записям.</p> <p>При подготовке необходимо выявлять наиболее сложные, дискуссионные вопросы, с тем, чтобы обсудить их с преподавателем на обзорных лекциях и консультациях. Нельзя ограничивать подготовку к экзамену простым повторением изученного материала. Необходимо углубить и расширить ранее приобретенные знания за счет новых идей и положений.</p> <p>Результат по сдаче зачета объявляется студентам, вносится в экзаменационную ведомость. Незачет проставляется только в ведомости.</p> <p>При получении незачета повторная сдача осуществляется в другие дни, установленные деканатом. Зачет выставляют, если студент усвоил учебный материал, исчерпывающе, логически, грамотно изложив его, показал знания специальной литературы, не допускал существенных неточностей, а также правильно применял понятийный аппарат.</p> <p>Готовиться к зачету необходимо последовательно, с учетом контрольных вопросов, разработанных преподавателем кафедры. Сначала следует определить место каждого контрольного вопроса в соответствующем разделе темы учебной программы, а затем внимательно прочитать и осмыслить рекомендованные научные работы, соответствующие разделы рекомендованных учебников. При этом полезно делать краткие выписки и заметки. Работу над темой можно считать завершенной, если вы сможете ответить на все контрольные вопросы и дать определение понятий по изучаемой теме.</p> <p>Для обеспечения полноты ответа на контрольные вопросы и лучшего запоминания теоретического материала рекомендуется составлять план ответа на контрольный вопрос. Это позволит сэкономить время для подготовки</p>

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

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

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

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

Компьютерный класс.

#### **12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья**

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:
- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;
- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по специальности: 10.05.03 "Информационная безопасность автоматизированных систем" и специализации "Безопасность открытых информационных систем".

*Приложение 2*  
*к рабочей программе дисциплины (модуля)*  
*Б1.О.30 Теоретические основы компьютерной безопасности*

**Перечень литературы, необходимой для освоения дисциплины (модуля)**

Специальность: 10.05.03 - Информационная безопасность автоматизированных систем

Специализация: Безопасность открытых информационных систем

Квалификация выпускника: специалист по защите информации

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2023

**Основная литература:**

1. Безопасность информационных систем [Электронный ресурс] / Ерохин В.В. - М.: ФЛИНТА, 2015. - 182 с. - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785976519046.html>
2. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. - М.: Книжный мир, 2009. - 352 с. - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785804103782.html>
3. Симметричные криптографические системы: учебно-методическое пособие по дисциплине 'Информационная безопасность' / Д.Р. Григорьева, Г.А. Гареева, Р.Р. Басыров - Набережные Челны: Изд-во НЧИ КФУ, 2018. - 30 с.

**Дополнительная литература:**

1. Информационная безопасность открытых систем [Электронный ресурс] / Мельников Д.А. - М.: ФЛИНТА, 2014. - 448 с. - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785976516137.html>
2. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону: Южный федеральный университет, 2016. - 74 с. - Режим доступа: <http://znanium.com/catalog/product/997105>
3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - Текст : электронный. - URL: <http://znanium.com/catalog/product/405000>

*Приложение 3  
к рабочей программе дисциплины (модуля)  
Б1.О.30 Теоретические основы компьютерной безопасности*

**Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем**

Специальность: 10.05.03 - Информационная безопасность автоматизированных систем

Специализация: Безопасность открытых информационных систем

Квалификация выпускника: специалист по защите информации

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2023

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.