**Министерство науки и высшего образования Российской Федерации**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Структурное подразделение «Институт информационных технологий и анализа данных»

**УТВЕРЖДЕНА:**
на заседании Совета института ИТиАД им. Е.И.Попова
Протокол №8 от 24 февраля 2025 г.

**Рабочая программа дисциплины**

# «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ»

Направление: 09.04.01 Информатика и вычислительная техника

Искусственный интеллект

Квалификация: Магистр

Форма обучения: очная

| | | |
|---|---|---|
| Документ подписан простой электронной подписью<br>Составитель программы: Маринов Александр Андреевич<br>Дата подписания: 19.06.2025 | Документ подписан простой электронной подписью<br>Утвердил: Говорков Алексей Сергеевич<br>Дата подписания: 19.06.2025 | Документ подписан простой электронной подписью<br>Согласовал: Афанасьев Александр Диомидович<br>Дата подписания: 19.06.2025 |

Год набора – 2025

Иркутск, 2025 г.

**1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы**

**1.1 Дисциплина «Информационная безопасность и защита данных» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения**

| Код, наименование компетенции | Код индикатора компетенции |
|---|---|
| ОПК-1 Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте | ОПК-1.5 |
| ОПК-5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем | ОПК-5.3 |
| ОПК-6 Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования | ОПК-6.1 |
| ОПК-8 Способен осуществлять эффективное управление разработкой программных средств и проектов | ОПК-8.2 |

**1.2 В результате освоения дисциплины у обучающихся должны быть сформированы**

| Код индикатора | Содержание индикатора | Результат обучения |
|---|---|---|
| ОПК-1.5 | Владеет навыками решения нестандартных профессиональных задач, с применением информационной безопасности и защиты данных в профессиональной деятельности | **Знать** методы информационной безопасности и защиты данных для использования в профессиональной деятельности.<br>**Уметь** решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде с применением информационной безопасности и защиты данных.<br>**Владеть** навыками теоретического и экспериментального исследования объектов профессиональной деятельности с применением технологий информационной безопасности и защиты данных, в том числе в новой или незнакомой среде. |
| ОПК-5.3 | Владеет навыками решения профессиональных задач, с применением информационной безопасности и защиты данных в профессиональной деятельности | **Знать** методы информационной безопасности и защиты данных для использования в профессиональной деятельности.<br>**Уметь** решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде |

| | | |
|---|---|---|
| | | с применением информационной безопасности и защиты данных.<br>**Владеть** навыками теоретического и экспериментального исследования объектов профессиональной деятельности с применением технологий информационной безопасности и защиты данных, в том числе в новой или незнакомой среде. |
| ОПК-6.1 | Владеет навыками решения профессиональных задач, с применением информационной безопасности и защиты данных в профессиональной деятельности | **Знать** методы информационной безопасности и защиты данных для использования в профессиональной деятельности.<br>**Уметь** решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде с применением информационной безопасности и защиты данных.<br>**Владеть** навыками теоретического и экспериментального исследования объектов профессиональной деятельности с применением технологий информационной безопасности и защиты данных, в том числе в новой или незнакомой среде. |
| ОПК-8.2 | Способен осуществлять эффективное управление разработкой программных средств и проектов | **Знать** методики эффективного управления разработкой программных средств и проектов<br>**Уметь** осуществлять эффективное управление разработкой программных средств и проектов<br>**Владеть** способами эффективного управления разработкой программных средств и проектов |

## 2 Место дисциплины в структуре ООП

Изучение дисциплины «Информационная безопасность и защита данных» базируется на результатах освоения следующих дисциплин/практик: «Специальные главы математики», «Технологии разработки программного обеспечения», «Компьютерные сети и телекоммуникационные системы»

Дисциплина является предшествующей для дисциплин/практик: «Производственная практика: преддипломная практика», «Интернет вещей», «Интеграция решений искусственного интеллекта в бизнес»

## 3 Объем дисциплины

Объем дисциплины составляет – 6 ЗЕТ

| **Вид учебной работы** | **Трудоемкость в академических часах** |
|---|---|

| | (Один академический час соответствует 45 минутам астрономического часа) | |
|---|---|---|
| | Всего | Семестр № 3 |
| Общая трудоемкость дисциплины | 216 | 216 |
| Аудиторные занятия, в том числе: | 42 | 42 |
| лекции | 14 | 14 |
| лабораторные работы | 28 | 28 |
| практические/семинарские занятия | 0 | 0 |
| Самостоятельная работа (в т.ч. курсовое проектирование) | 138 | 138 |
| Трудоемкость промежуточной аттестации | 36 | 36 |
| Вид промежуточной аттестации (итогового контроля по дисциплине) | Экзамен | Экзамен |

## 4 Структура и содержание дисциплины

### 4.1 Сводные данные по содержанию дисциплины

**Семестр № 3**

| № п/п | Наименование раздела и темы дисциплины | Виды контактной работы | | | | | | СРС | | Форма текущего контроля |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Лекции | | ЛР | | ПЗ(СЕМ) | | | | |
| | | № | Кол. Час. | № | Кол. Час. | № | Кол. Час. | № | Кол. Час. | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1 | Доступность информации | 1 | 2 | 1 | 3 | | | 2 | 14 | Устный опрос |
| 2 | Целостность информации | 2 | 2 | 2 | 4 | | | 2 | 25 | Доклад |
| 3 | Конфиденциальность информации | 3 | 2 | 3 | 4 | | | 1 | 24 | Доклад |
| 4 | Объекты защиты | 4 | 2 | 4 | 4 | | | 1 | 16 | Доклад |
| 5 | ФЗ "Об информации, информационных технологиях и о защите информации" | 5 | 2 | 5 | 3 | | | 1 | 14 | Доклад |
| 6 | Категории и носители информации | 6 | 1 | 6 | 3 | | | 2 | 12 | Устный опрос |
| 7 | Угрозы информации | 7 | 1 | 7 | 3 | | | 1 | 18 | Устный опрос |
| 8 | Средства защиты информации | 8 | 2 | 8 | 4 | | | 2 | 15 | Доклад |
| | Промежуточная аттестация | | | | | | | | 36 | Экзамен |
| | Всего | | 14 | | 28 | | | | 174 | |

### 4.2 **Краткое содержание разделов и тем занятий**

**Семестр № 3**

| № | Тема | Краткое содержание |
|---|---|---|

| | | |
|---|---|---|
| 1 | Доступность информации | рассматривается свойство системы для обеспечения своевременногобеспрепятственного доступа правомочных (авторизованных) субъектов к интересующей ихинформации или осуществлять своевременный информационный обмен между ними.Безопасные информационные системы создаются (приобретаются) для получения определенныхинформационных услуг. Если по тем или иным причинам предоставить эти услугипользователям становится невозможно, это, очевидно, наносит ущерб всем субъектаминформационных отношений. Особенно ярко ведущая роль доступности проявляется вразного рода системах управления – производством, транспортом и т.п. Внешне менеедраматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуетсябольшое количество людей (продажа железнодорожных и авиабилетов, банковские услугии т.п.). |
| 2 | Целостность информации | рассматривается свойство информации, характеризующее ее устойчивостьк случайному или преднамеренному разрушению или несанкционированному изменению.Целостность можно подразделить на статическую (понимаемую как неизменностьинформационных объектов) и динамическую (относящуюся к корректному выполнениюсложных действий (транзакций)). Средства контроля динамической целостностиприменяются, в частности, при анализе потока финансовых сообщений с целью выявлениякражи, переупорядочения или дублирования отдельных сообщений. Целостностьоказывается важнейшим аспектом информационной безопасности в тех случаях, когдаинформация служит «руководством к действию». |
| 3 | Конфиденциальность информации | рассматривается свойство информации быть известной идоступной только правомочным субъектам системы (пользователям, программам,процессам). Конфиденциальность – самый проработанный у нас в стране аспектинформационной безопасности. К сожалению, практическая реализация мер пообеспечению конфиденциальности современных информационных систем наталкивается вРоссии на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей |

| | | |
|---|---|---|
| | | лишеновозможности составить представление о потенциальных рисках. Во-вторых, на путипользовательской криптографии как основного средства обеспечения конфиденциальностистоят многочисленные законодательные препоны и технические проблемы. |
| 4 | Объекты защиты | рассматриваются основные объекты защиты при обеспечении информационной безопасности:- все виды информационных ресурсов (документированнаяинформация) - информация, зафиксированная на материальном носителе с реквизитами,позволяющими ее идентифицировать;- права граждан, юридических лиц и государства на получение, распространение ииспользование информации;- система формирования, распространения и использования информации (информационныесистемы и технологии, библиотеки, архивы, персонал, нормативные документы и т.д.);- система формирования общественного сознания (СМИ, социальные институты и т.д.). |
| 5 | ФЗ "Об информации, информационных технологиях и о защите информации" | рассматривается российское законодательство (базовые законы) в области защиты информации, ФЗ "Об информации, информационных технологиях и о защите информации". Студенты изучают основные понятия и решения, закрепленные взаконе, которые требуют пристального рассмотрения. Особое внимание уделяется следующим отношениям, возникающим при: - осуществлении права на поиск, получение, передачу, производство и распространение информации;- применении информационных технологий;- обеспечении защиты информации (данных). |
| 6 | Категории и носители информации | рассматривается информация, правовые режимы в рамках которой установлено действующее законодательство в областигосударственной, коммерческой, промышленной и другой общественной деятельности. Указы Президента РФ. |
| 7 | Угрозы информации | в материале рассматривается получение лицами в обход системы защиты с помощью программных, технических и других средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации, а также бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена. |
| 8 | Средства защиты | практическая работа ведется на примерах средств |

| | | |
|---|---|---|
| | информации | защиты: формальные средства защиты; физические средства; аппаратные средства; Программные средства; специфические средства;неформальные средства защиты. Данный подход помогает сформировать у обучающихся важные компетенции в области политику информационной безопасности и освоить: программно-технические способы и средства обеспечения информационной безопасности;обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных. |

**4.3 Перечень лабораторных работ**

**Семестр № 3**

| № | Наименование лабораторной работы | Кол-во академических часов |
|---|---|---|
| 1 | обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации | 3 |
| 2 | Рассмотреть свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению | 4 |
| 3 | Рассмотреть свойство информации быть известной и доступной только правомочным субъектам системы (пользователям, программам, процессам) | 4 |
| 4 | Работа с основными объектами защиты при обеспечении информационной безопасности | 4 |
| 5 | Основные понятия и практические решения, закрепленные в ФЗ | 3 |
| 6 | Информация, запрещенная к распространению | 3 |
| 7 | Непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию | 3 |
| 8 | Практическое описание технологии защиты информации конкретной информационной системы | 4 |

**4.4 Перечень практических занятий**

Практических занятий не предусмотрено

**4.5 Самостоятельная работа**

**Семестр № 3**

| № | Вид СРС | Кол-во академических часов |
|---|---|---|

| | | |
|---|---|---|
| 1 | Подготовка презентаций | 72 |
| 2 | Решение специальных задач | 66 |

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: В ходе проведения лекций и практических работ используются следующие интерактивные методы обучения, основанные на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

## 5 Перечень учебно-методического обеспечения дисциплины

### 5.1 Методические указания для обучающихся по освоению дисциплины

#### 5.1.1 Методические указания для обучающихся по лабораторным работам:

Практические работы направлены на изучение содержания дисциплины, технологии оценки экономических показателей инфраструктуры информационной безопасности на основе решения ряда узловых задач в приложении к конкретным проектам в сфере будущей профессиональной деятельности.
Ход работы (при выполнении заданий по лабораторным работам):
1) Из предложенных преподавателем направлений возможных задач каждый студент формулирует интересующую его тему конкретного проекта, которая может быть связана или с предстоящей темой выпускной квалификационной работы, или с самостоятельным замыслом реализации интересующего проекта или с разработкой некоторого проекта в связи с участием в научной или производственной деятельности.
2) Для выполнения работ студентам предлагается перечень задач, которые должны быть решены каждым студентом под свою тему проекта.
3) Порядок осуществления решения каждой задачи включает:
- ознакомление в курсе лекций и рекомендуемой литературе с постановкой и методом решения каждой из перечисленных задач;
- проработку решения задач под избранную тему проекта, используя известные типовые или аналогичные варианты решения задач.

5.1 Методические указания для обучающихся по освоению дисциплины:
5.1.1 Методические указания для обучающихся по лабораторным работам:
Практические работы направлены на изучение содержания дисциплины, технологии оценки экономических показателей инфраструктуры информационной безопасности на основе решения ряда узловых задач в приложении к конкретным проектам в сфере будущей профессиональной деятельности.
Ход работы (при выполнении заданий по лабораторным работам):
1) Из предложенных преподавателем направлений возможных задач каждый студент формулирует интересующую его тему конкретного проекта, которая может быть связана или с предстоящей темой выпускной квалификационной работы, или с самостоятельным замыслом реализации интересующего проекта или с разработкой некоторого проекта в связи с участием в научной или производственной деятельности.
2) Для выполнения работ студентам предлагается перечень задач, которые должны быть решены каждым студентом под свою тему проекта.
3) Порядок осуществления решения каждой задачи включает:

- ознакомление в курсе лекций и рекомендуемой литературе с постановкой и методом решения каждой из перечисленных задач;
- проработку решения задач под избранную тему проекта, используя известные типовые или аналогичные варианты решения задач.
4) Решение задач сопровождается поддержкой программного продукта, которого студент выбирает из числа свободных программного обеспечения или обеспечиваемого из имеющихся по лицензиям университета (Microsoft Office и др.)
5) Результаты решения всех задач описываются согласно требованиям действующего стандарта ИРНИТУ СТО 005-2020.
https://el.istu.edu/course/index.php?categoryid=1107

**5.1.2 Методические указания для обучающихся по самостоятельной работе:**

Практические работы направлены на освоение арсенала методов (основ теории) для решения задач по дисциплине.
Ход работы (при выполнении заданий по практическим работам):
1) Ознакомиться по материалам курса лекций, по литературе или другим источникам информации с методами оценки экономических показателей;
2) Отыскать решение данных задач для конкретных случаев;
3) Сделать необходимые заготовки материалов (провести описание привлекаемых к решениям методов) для дальнейшего выполнения работ в приложении к своему проекту;
4) Теоретические основы и примеры решения задач могут представляться в качестве образцовых для заслушивания и обсуждения аудиторией.
https://el.istu.edu/course/index.php?categoryid=1107

## 6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

### 6.1 Оценочные средства для проведения текущего контроля

#### 6.1.1 семестр 3 | Устный опрос

**Описание процедуры.**

Проведение устного опроса в форме «вопрос-ответ»

**Критерии оценивания.**

ответ раскрыт полностью 8-10 баллов
ответ раскрыт частично 4-7 баллов
имеет только общее представление о проблеме 2-4 баллов
не ответил – 0 баллов

#### 6.1.2 семестр 3 | Доклад

**Описание процедуры.**

Студент должен составить математическую модель распространения и использования информации (информационные системы и технологии, библиотеки, архивы, персонал, нормативные документы и т.д.).

**Критерии оценивания.**

Ответы на устный опрос оцениваются «зачтено» или «незачтено». Оценка «зачтено» ставится, если студент раскрыл вопрос в полном объеме. Оценка «незачтено» ставится в случае, если студент не смог раскрыть поставленный вопрос.

### 6.2 Оценочные средства для проведения промежуточной аттестации

#### 6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

| Индикатор достижения компетенции | Критерии оценивания | Средства (методы) оценивания промежуточной аттестации |
|---|---|---|
| ОПК-1.5 | отлично<br>хорошо<br>удовлетворительно<br>неудовлетворительно | Устное собеседование по теоретическим вопросам, практико-ориентированные задания,дискуссия. |
| ОПК-5.3 | отлично<br>хорошо<br>удовлетворительно<br>неудовлетворительно | Устное собеседование по теоретическим вопросам, практико-ориентированные задания,дискуссия. |
| ОПК-6.1 | отлично<br>хорошо<br>удовлетворительно<br>неудовлетворительно | Устное собеседование по теоретическим вопросам, практико-ориентированные задания,дискуссия. |
| ОПК-8.2 | отлично<br>хорошо<br>удовлетворительно<br>неудовлетворительно | Устное собеседование по теоретическим вопросам, практико-ориентированные задания,дискуссия. |

#### 6.2.2 Типовые оценочные средства промежуточной аттестации

### 6.2.2.1 Семестр 3, Типовые оценочные средства для проведения экзамена по дисциплине

#### 6.2.2.1.1 Описание процедуры

семинарских занятиях, защищенные студентом.
1) Экзамен по дисциплине проводится согласно расписанию в назначенной аудитории, в которую приглашается к установленному началу экзамена группа студентов.
2) К экзамену допускаются студенты, которые выполнили все предусмотренные работы по освоению курса: сданы практические работы по выбранной теме.
3). Каждый студент из числа допущенных выбирает один билет и готовится к ответу в течение не менее 30 - 45 минут письменно на поставленные три вопроса в билете.
Во время экзамена для оценки знаний используются следующие вопросы:
1. Система обеспечения информационной безопасности.
2. Обеспечение информационной безопасности объектов КИИ.
3. Обеспечение информационной безопасности Российской Федерации.
4. Содержание и структура законодательства. Законодательство об информации, информационных технологиях и о защите информации.
5. Термины и определения в области защиты информации.
6. Государственной системы защиты информации.
7. Задачи органов Государственной системы защиты информации.
8. Административная и уголовная ответственность в сфере защиты информации
9. Персональные данных, их классификация
10. Принципы обработки персональных данных.
11. Создания и оценка соответствия информационной системы персональных данных.
12. Обязанности оператора при обработке персональных данных.
13. Задачи, методы и средства защиты информации.
14. Понятие уязвимости и угрозы информации.
15. Источники утраты конфиденциальности и искажения информации.
16. Понятие и виды информационных ресурсов. Информационные ресурсы государственного значения.
17. Понятие конфиденциальности. Критерии выделения информации ограниченного распространения.
18. Понятие информационного противоборства, его формы и методы.
19. Понятие преступления в информационной сфере.
20. Характеристика основных составов преступлений, связанных с информационными отношениями.
21. Угрозы безопасности информации в процессе использования компьютеров, локальных сетей и средств связи.
22. Правовое регулирование информационных отношений в сети Интернет, обеспечение защиты информационных ресурсов в глобальной информационной сети.
23. Виды охраняемых объектов, категории защищаемых помещений. Задачи и направления охраны объектов.
24. Защита конфиденциальной информации в условиях экстремальных (чрезвычайных) ситуаций.
25. Правовой режим государственной тайны.
26. Правовой режим служебной тайны.
27. Международное сотрудничество в области информационной безопасности и защиты информации.
28. Профессиональные тайны как вид информации ограниченного распространения, особенности их правового режима (создание модели).
29. Особенности правового режима личной тайны, обеспечение тайны переписки,

телефонных переговоров и иных сообщений (создание модели).
30. Понятие и правовой режим персональных данных (создание модели).
31. Понятие и виды организационных мер обеспечения информационной безопасности и защиты информации (создание модели).
32. Анализ и оценка угроз информационной безопасности объекта.
33. Организация обеспечения режима конфиденциальности на объекте.
34. Регламентация допуска и доступа персонала к конфиденциальной информации.
35. Служба безопасности, её структура и задачи по обеспечению информационной безопасности.
36. Задачи и способы подбора персонала на работу, связанную с использованием конфиденциальной информации.
37. Организация работы с персоналом, допущенным к конфиденциальной информации.
38. Предупредительные и профилактические меры, направленные на предотвращение разглашения персоналом конфиденциальной информации.
Организация защиты информации при подготовке и проведении совещаний.
39. Организация защиты информации при проведении переговоров.
40. Защита информации в процессе научной, рекламной и выставочной деятельности.
41. Защита конфиденциальных сведений при работе с клиентами и посетителями.
42. Понятие и виды технических мер обеспечения информационной безопасности и защиты информации.
43. Виды угроз информационной безопасности, исходящих по техническим каналам.
44. Средства и методы технической защиты объектов и информации.

Пример задания:

1. Основные нормативно-правовые акты в области защиты персональных данных.
2. Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных.
3. Разграничение и контроль доступа к персональным данным.

**6.2.2.1.2 Критерии оценивания**

| **Отлично** | **Хорошо** | **Удовлетворительно** | **Неудовлетворительно** |
|---|---|---|---|
| На высоком уровне демонстрирует знание основных методик защиты информации и их практическое применение; владение навыками обеспечения информационной безопасности; знание классификации угроз информационной | С незначительными неточностями демонстрирует знание основных методик защиты информации и их практическое применение; умение определять возможные источники угроз информационной безопасности; владение навыками обеспечения | Частично демонстрирует знание основных методик защиты информации и их практическое применение; умение определять возможные источники угроз информационной и экономической безопасности хозяйствующих субъектов; владение навыками обеспечения | Демонстрирует отсутствие знания основных методик защиты информации и их практическое применение; умение определять возможные источники угроз информационной безопасности хозяйствующих субъектов; владение навыками обеспечения информационной и экономической безопасности; знание классификации угроз |

| | | | |
|---|---|---|---|
| безопасности; умение использовать специализированное программное обеспечение для информационной защиты; владение навыками осуществлять организацию информационной защиты, охраны интеллектуальной собственности с использованием технических и программных средств. | информационной и экономической безопасности; знание классификации угроз информационной безопасности; умение использовать специализированное программное обеспечение для информационной защиты. | информационной и экономической безопасности; знание классификации угроз экономической и информационной безопасности; умение использовать специализированное программное обеспечение для информационной защиты; владение навыками осуществлять организацию информационной защиты, охраны интеллектуальной собственности с использованием технических и программных средств. | экономической и информационной безопасности; умение использовать специализированное программное обеспечение для информационной защиты; владение навыками осуществлять организацию информационной защиты, охраны интеллектуальной собственности с использованием технических и программных средств. |

7 **Основная учебная литература**

1. Глухих В. И. Информационная безопасность и защита данных : учебное пособие / В. И. Глухих, 2012. - 244.

2. Информационная безопасность и защита информации : учебное пособие для вузов по направлению "Информационные системы и технологии" / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова, Н. Г. Шахов, 2016. - 383.

**8 Дополнительная учебная литература и справочная**

1. Мельников В. П. Информационная безопасность и защита информации : учебное пособие для студентов высшего профессионального образования ; под ред. С. А. Клейменова / В. П. Мельников, С. А. Клейменов, А. М. Петраков, 2011. - 336.

2. Технологии Электронных Коммуникаций [Текст]. Т. 62 : Модемы: разработка и использование в России, 1996. - 76.

3. Платонов В. В. Программно-аппаратные средства защиты информации : учебник для вузов по направлению "Информационная безопасность" / В. В. Платонов, 2013. - 330.

**9 Ресурсы сети Интернет**

1. http://library.istu.edu/
2. https://e.lanbook.com/

**10 Профессиональные базы данных**

1. http://new.fips.ru/
2. http://www1.fips.ru/

**11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем**

1. Microsoft Windows Seven Professional (Microsoft Windows Seven Starter) - Seven, Vista, XP_prof_64, XP_prof_32 - поставка 2010

2. Microsoft Windows Seven Professional [1x100] RUS (проведен апгрейд с Microsoft Windows Seven Starter [1x100]) - поставка 2010

3. Microsoft Windows Server Standard 2008 R2 Russian Academic OPEN 1 License No Level

**12 Материально-техническое обеспечение дисциплины**

1. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

2. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

3. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

4. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

5. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

6. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

7. МФУ FS-1128 MFP

8. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

9. Сервер CPU Intel Core i7-960/GA-X58A-UD3R/DDR-IIIDimm 2Gb/HDD 1 Tb/DVD-RW/512MB PCI-E/блок пит.+ПО

10. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

11. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

12. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

13. Проектор Epson EB-W04LCD.WXGA 1280*800.3000:1.2800 ANSI Lumens