Федеральное государственное образовательное бюджетное учреждение

высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ**

**ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**(Финансовый университет)**

**Кафедра информационной безопасности**

**Факультета информационных технологий и анализа больших данных**

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Проректор по учебной и  методической работе  \_\_\_\_\_\_\_\_\_\_\_\_Е. А. Каменева  « 28 » мая 2024 г. |

**С.Л. Ларионова**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭКОНОМИЧЕСКИХ СИСТЕМ**

**Рабочая программа дисциплины**

для студентов, обучающихся по направлению подготовки

38.03.01 «Экономика»

Образовательная программа «Финансовая разведка, управление рисками и экономическая безопасность»,

Образовательная программа «Экономика и бизнес»,

Образовательная программа «Корпоративные финансы»

*Рекомендовано Ученым советом Факультета*

*информационных технологий и анализа больших данных*

*(протокол от «21» мая 2024 г. № 44)*

*Одобрено на заседании Кафедры информационной безопасности*

*(протокол от «25» апреля 2024г. №3)*

Москва 2024

**СОДЕРЖАНИЕ**

[1.Наименование дисциплины 5](#_Toc532737989)

[2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине 5](#_Toc532737990)

[3. Место дисциплины в структуре образовательной программы 6](#_Toc532737991)

[4. Объем дисциплины(модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся 6](#_Toc532737992)

[5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий 6](#_Toc532737993)

[5.1. Содержание дисциплины 6](#_Toc532737994)

[5.2. Учебно-тематический план 7](#_Toc532737995)

[5.3. Содержание семинаров, практических занятий 10](#_Toc532737996)

[6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине 10](#_Toc532737997)

[6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы 10](#_Toc532737998)

[6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю 11](#_Toc532737999)

[7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине 14](#_Toc532738000)

[8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 22](#_Toc532738004)

[9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины 24](#_Toc532738005)

[10. Методические указания для обучающихся по освоению дисциплины 24](#_Toc532738006)

[11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем . 25](#_Toc532738007)

[11.1. Комплект лицензионного программного обеспечения: 25](#_Toc532738008)

[11.2 Современные профессиональные базы данных и информационные справочные системы: 25](#_Toc532738009)

[11.3 Сертифицированные программные и аппаратные средства защиты информации. 25](#_Toc532738010)

[12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине. 25](#_Toc532738011)

# 1.Наименование дисциплины

«Информационная безопасность экономических систем».

**2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине**

|  |  |  |  |
| --- | --- | --- | --- |
| Код компе-тенции | Наименование компетенции | Индикаторы достижения компетенции | Результаты обучения (умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции |
| ПКН-6 | Способность предлагать решения профессиональных задач в меняющихся финансово-экономических условиях. | 1. Понимает содержание и логику проведения анализа деятельности экономического субъекта, приемы обоснования оперативных, тактических и стратегических управленческих решений | **Знать** логику проведения анализа деятельности экономического субъекта, приемы обоснования оперативных, тактических и стратегических управленческих решений  **Уметь** проводить анализ деятельности экономического субъекта, обосновывать оперативные, тактические и стратегические управленческие решения |
| 2. Предлагает варианты решения профессиональных задач в условиях неопределенности | **Знать** методы решения профессиональных задач в условиях неопределенности  **Уметь** разрабатывать и предлагать варианты решения профессиональных задач в условиях неопределенности |
| УК-15 | Способность релевантно решаемым задачам использовать информационные ресурсы и информационно-коммуникационные технологии для достижения целей, связанных с профессиональной деятельностью, обучением, участием в жизни общества и других сферах жизни | 1. Самостоятельно выбирает и использует цифровые средства общения, осуществляет поиск и/или создание контента в соответствии с целью взаимодействия, в том числе для организации совместной деятельности. | **Знать** цифровые средства общения с целью взаимодействия, в том числе для организации совместной деятельности.  **Уметь** самостоятельно выбирать и использовать цифровые средства общения, осуществлять поиск и/или создание контента в соответствии с целью взаимодействия, в том числе для организации совместной деятельности. |
|  | 1. Владеет навыками организации взаимодействия и коммуникации с помощью информационных систем и/или цифровых сервисов и технологий. | **Знать**  способы организации взаимодействия и коммуникации с помощью информационных систем и/или цифровых сервисов и технологий.  **Уметь** организовывать взаимодействие и коммуникации с помощью информационных систем и/или цифровых сервисов и технологий, осуществлять подбор и применение различных информационно-коммуникационных средств для решения образовательных и профессиональных задач. |
|  | 3.  Осуществляет подбор и применение различных информационно-коммуникационных средств для решения образовательных и профессиональных задач. | **Знать** информационно-коммуникационные средства для решения образовательных и профессиональных задач.  **Уметь** осуществлять подбор и применение различных информационно-коммуникационных средств для решения образовательных и профессиональных задач. |

**3. Место дисциплины в структуре образовательной программы**

Дисциплина "Информационная безопасность экономических систем" является дисциплиной по выбору цикла профиля (элективный).

**4. Объем дисциплины(модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся**

Таблица 1

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы по дисциплине** | **Всего**  **(в з/е и часах)** | **Семестр 6**  **(в часах)** |
| **Общая трудоемкость дисциплины** | **3 з.е., 108 ч.** | **3 з.е., 108 ч.** |
| ***Контактная работа - Аудиторные занятия*** | ***34*** | ***34*** |
| *Лекции* | ***16*** | ***16*** |
| *Семинары, практические занятия* | ***18*** | ***18*** |
| ***Самостоятельная работа*** | ***74*** | ***74*** |
| Вид текущего контроля | контрольная работа | контрольная работа |
| Вид промежуточной аттестации | зачет | зачет |

**5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий**

**5.1. Содержание дисциплины**

**Тема 1. Классификация и типы экономических информационных систем.** Экономический процесс и экономическая информация. Понятие экономической информационной системы. Технология и методы обработки экономической информации. Телекоммуникационные технологии в экономических информационных системах. Классификация информационных экономических систем. Учетные системы и расчетные системы. Статистические информационные системы. Бухгалтерские системы. Банковские системы. Системы комплексной автоматизации хозяйственной деятельности промышленных предприятий.

**Тема 2. Оценка защищенности экономических систем.** Существующиестандарты и методологии проверки и оценки защищенности ИТ и СУИБ: их отличия, сильные и слабые стороны. Международный стандарт оценки защищенности ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011. Базовые вопросы проверки защищенности. Оценка эффективности и результативности деятельности поуправлению ИБ. Измерение, мера измерения, показатель и метрика. Метрики безопасности. Системы анализа защищенности.

**Тема 3. Конкурентная разведка.**

Конкурентная разведка, цели и задачи. Методы выявления и анализа конкурирующих фирм. Понятие и содержание конкуренции в предпринимательской сфере. Создание подразделений конкурентной разведки на предприятии. Интернет-разведка – как инструмент конкурентной разведки. Методы и приемы информационно-аналитической обработки информации о юридическом и физическом лицах - потенциальных объектах информационной угрозы безопасности предприятия.

**Тема 4. Организация системы защиты информации экономических систем.**

Этапы построения системы защиты информации. Политика безопасности. Оценка эффективности инвестиций в информационную безопасность. Обеспечение компьютерной безопасности учетной информации. Информационная безопасность электронной коммерции (ЭК). Обеспечение информационной безопасности автоматизированных банковских систем (АБС).

**5.2. Учебно – тематический план**

| **№ п/п** | **Наименование тем (разделов)**  **дисциплины,** | **Трудоемкость в часах** | | | | |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Все-го** | **Контактная работа\* - Аудиторная работа** | | | **Самосто-ятельная**  **работа** | **Формы текущего контроля успеваемости** |
| Общая,  в т.ч.: | Лекции | Семинары, практи-ческие занятия |
| 1. | Классифика-ция и типы экономических информацион-ных систем | 26 | 8 | 4 | 4 | 18 | Доклады, презентации, обсуждение в группе, письменная проверочная работа |
| 2. | Оценка защищенности экономических систем | 26 | 8 | 4 | 4 | 18 | Доклады, презентации, обсуждение в группе, опрос, решение ситуационной задачи, письменная проверочная работа |
| 3. | Конкурентная разведка | 26 | 8 | 4 | 4 | 18 | Доклады, презентации, решение ситуационной задачи, письменная проверочная работа |
| 4. | Организация системы защиты информации экономических систем | 30 | 10 | 4 | 6 | 20 | Доклады, презентации, решение ситуационной задачи, письменная проверочная работа |
|  | В целом по дисциплине | 108 | 34 | 16 | 18 | 74 | Согласно учебному плану:  Контрольная работа |
|  | Итого в % |  | 31 | 47 | 53 | 69 |  |

\*Объем контактной работы в очно-заочной/заочной формах обучения и индивидуальных учебных планах определяется соответствующими учебными планами. Темы, реализуемые в виде контактной работы, определяются преподавателем самостоятельно, исходя из уровня их сложности.

5.3. Содержание семинаров, практических занятий

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **темы** | **Наименование тем (разделов) дисциплины** | **Перечень вопросов для обсуждения на семинарах, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)** | **Формы проведения занятий** |
|  | Классификация и типы экономических информационных систем | 1. Назначение, функции, данные, сетевая архитектура учетных систем, уровень защищенности. 2. Расчетные системы: назначение, функции и сети передачи данных. Классификация по уровню защищенности. 3. Назначение, данные, архитектура, уровень защищенности статистических систем. 4. Банковские системы: типы данных, функции, удаленный доступ, уровень защищенности.   Решение задач классификации по уровню защищенности  Источники: 8.12, 8.13, 9.2, 9.3, 9.4 | Дискуссии.  Презентации  Обсуждение индивидуальных заданий  Учебное практическое задание: классификация по уровню защищенности системы ведения счетов клиентов  Учебное практическое задание: классификация по уровню защищенности системы передачи сообщений между кредитными организациями SWIFT по уровню защищенности. |
|  | Оценка защищенности экономических систем | 1. Методы оценка эффективности деятельности по управлению ИБ. 2. Показатели оценки эффективности управления ИБ.   3.Оценка эффекта защиты и целесообразности применения мер защиты.  4. Системы анализа защищенности.  Решение задач определения уровня защищенности, расчета показателей эффективности и эффекта защиты.  Источники: 8.5., 8.7., 8.10, 8.11, 8.14, 9.1., 9.2, 9.3, 9.7, 9.8 | Дискуссии, Презентации, Обсуждение индивидуальных заданий.  Учебное практическое задание:  Практическое учебное задание: подсчитать время простоя системы, работающий в режиме 24х7 365 дней в году, если показатель доступности составил 98%.  Учебное практическое задание:  Рассчитать эффект защиты, если риск до защиты составил 1500, а риск после защиты составил 1000. |
|  | Конкурентная разведка | 1. Цели конкурентной разведки в банковских системах. Уязвимости и угрозы систем. 2. Цели конкурентной разведки учетных систем. Уязвимости и угрозы. 3. Системы обеспечения хозяйственной деятельности предприятия. Уязвимости и угрозы.   Источники: 8.13, 8.15, 9.4, 9.6. | Дискуссии, Презентации, Обсуждение индивидуальных заданий  Ситуационное задание: Рассматривается система ведения отношений с клиентами в банке. Определите цели и методы конкурентной разведки.  Учебное практическое задание: Определите угрозы и уязвимости системы ведения счетов физических лиц, доступ к которой обеспечен через интернет. |
|  | Организация системы защиты информации экономических систем | 1. Политика информационной безопасности учетных систем. 2. Политика информационной безопасности банковских систем. 3. Политика информационной безопасности систем электронной коммерции.   Источники: 8.1., 8.2., 8.3., 8.6., 8.12, 9.2, 9.7, 9.8, 9.9. | Дискуссии, Презентации,  Обсуждение индивидуальных заданий  Учебное практическое задание: Разработайте политику информационной безопасности для системы управления счетами клиентов-юридических лиц.  Ситуационное задание: Если к системе управления счетами клиентов обеспечен доступ через Интернет, определите методы и средства защиты системы. |

**6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

**6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы**

| **Наименование тем (разделов) дисциплины** | **Перечень вопросов, отводимых на самостоятельное освоение** | **Формы внеаудиторной самостоятельной работы** |
| --- | --- | --- |
| Классификация и типы экономических информационных систем | Базовые вопросы проверки защищенности ИБ.  Процессный подход к разработке, реализации, эксплуатации, сопровождения и совершенствования процессов проверки защищенности экономических систем. Виды проверок.  Самооценка ИБ. | - работа с учебной, научной и справочной литературой;  - конспект;  - подготовка докладов по теме;  - подготовка презентаций по теме;  - выполнение учебного задания |
| Оценка защищенности экономических систем | Функции экономических систем и среда функционирования.  Оценка уровня защищенности экономических систем.  Расчет эффективности мер защиты информации. | - работа с учебной, научной и справочной литературой;  - конспект;  - подготовка докладов по теме;  - подготовка презентаций по теме;  - выполнение учебного задания |
| Конкурентная разведка | Методы и приемы конкурентной разведки.  Уязвимости экономических систем.  Методы противодействия конкурентной разведке. | - работа с учебной, научной и справочной литературой;  - конспект;  - подготовка докладов по теме;  - подготовка презентаций по теме;  - выполнение учебного задания |
| Организация системы защиты информации экономических систем | Подходы к организации защиты информации в информационных системах.  Особенности экономических систем. Требования к обеспечению информационной безопасности.  Организация обеспечения информационной безопасности экономических систем разного назначения. | - работа с учебной, научной и справочной литературой;  - конспект;  - подготовка докладов по теме;  - подготовка презентаций по теме;  - выполнение учебного задания |

**6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю**

**Примерный перечень вопросов к контрольной работе, примеры заданий контрольных работ:**

* Содержание деятельности по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности. Принципы и форма деятельности по обеспечению информационной безопасности.
* Методы и средства деятельности по обеспечению информационной безопасности. Субъекты обеспечения информационной безопасности.
* Нормативная база обеспечения информационной безопасности информационных систем.
* Модель информационной безопасности бизнеса. Ущерб и негативные последствия нарушения обеспечения информационной безопасности. Оценка последствий нарушения ИБ. Риски ИБ в организациях.
* Международные стандарты управления обеспечением информационной безопасности.
* Способы оценки информационной безопасности. Типовые модели оценки информационной безопасности на основе оценки процессов.
* Оценка эффективности методов и средств защиты информации.
* Типовые угрозы ИБ от персонала и методы противодействия угрозам ИБ от персонала.
* Модель злоумышленника-сотрудника.
* Жизненный цикл ИТ-технологий. Формирование стоимости владения информационным активом.
* Оценка уровней критичности информационного актива. Структура информационного риска. Методика анализа риска информационной безопасности.
* Формирование политики безопасности организации.
* Классификация информационных систем по уровням защищенности.
* Законодательные акты Российской Федерации в области защиты информации и обеспечения информационной безопасности.
* Комплексная защита информационных систем.
* Организация защиты программного обеспечения от исследования.

**Примерные темы индивидуальных заданий:**

1. Международные стандарты и лучшие практики оценки защищенности информационных систем.
2. Назначение, функции, виды обрабатываемых данных, среда функционирования автоматизированной системы обработки бэк-офисных банковских операций. Угрозы и уязвимости систем.
3. Назначение, функции, виды обрабатываемых данных, среда функционирования автоматизированной системы обработки систем бухгалтерского учета предприятия. Угрозы и уязвимости систем.
4. Назначение, функции, виды обрабатываемых данных, среда функционирования автоматизированной системы обработки систем удаленного доступа к счетам физических лиц. Угрозы и уязвимости систем.
5. Организация информационной безопасности автоматизированных систем управления предприятием.
6. Организация информационной безопасности автоматизированных систем складского учета.
7. Организация информационной безопасности систем ведения кадрового учета.

**Примерная тематика для дискуссий:**

1. Стандартизация в области оценки защищенности ИТ и деятельности по управлению ИБ – история разработки нормативной базы и сравнение международных стандартов и лучших практик в данной области.
2. Детальная разработка процессов проверки защищенности экономических систем.
3. Организация конкурентной разведки по добыванию сведений в экономических системах.
4. Разработка показателей эффективности и результативности процессов обеспечения информационной безопасности экономических систем.
5. Описание функционала различных инструментальных систем проверки и оценки защищенности информационных систем и деятельности по управлению информационной безопасности экономических систем.
6. Политика информационной безопасности систем электронной коммерции.
7. Политика информационной безопасности систем дистанционного банковского обслуживания.
8. Политика информационной безопасности систем управления счетами физических лиц.

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях Кафедры информационной безопасности.

**7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине**

Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине содержится в разделе «2.Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

**Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, владений**

Таблица 5

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование компетенции | Наименование индикаторов достижения компетенции | Результаты обучения ( умения и знания), соотнесенные с индикаторами достижения компетенции | Типовые контрольные задания |
| **ПКН-6.** Способность предлагать решения профессиональных задач в меняющихся финансово-экономических условиях. | **Индикатор 1.** Понимает содержание и логику проведения анализа деятельности экономического субъекта, приемы обоснования оперативных, тактических и стратегических управленческих решений | **Знать** логику проведения анализа деятельности экономического субъекта, приемы обоснования оперативных, тактических и стратегических управленческих решений  **Уметь** проводить анализ деятельности экономического субъекта, обосновывать оперативные, тактические и стратегические управленческие решения | **Задание 1.** Перечислите основные способы проведения аудита объектов и систем на соответствие требованиям стандартов в области управления информационной безопасности. Кратко определите содержание каждого способа.  **Задание 2.** Разработайте инструкцию по организации управления обеспечения информационной безопасности на основе международных стандартов ИСО27000. Укажите номера и названия использованных стандартов. |
| **Индикатор 2.** Предлагает варианты решения профессиональных задач в условиях неопределенности | **Знать** методы решения профессиональных задач в условиях неопределенности  **Уметь** разрабатывать и предлагать варианты решения профессиональных задач в условиях неопределенности | **Задание 1.** Приведите и обоснуйте средства и подсистемы обеспечения информационной безопасности внутри банковской системы ведения счетов физических лиц.  **Задание 2.** Определить целесообразность использования антивируса для защиты, если риск заражения вирусом до защиты составил 2000 руб, риск после защиты снизился в 10 раз, стоимость антивируса составила 1000 руб |
| **УК-15.** Способность релевантно решаемым задачам использовать информационные ресурсы и информационно-коммуникационные технологии для достижения целей, связанных с профессиональной деятельностью, обучением, участием в жизни общества и других сферах жизни | **Индикатор 1.** Самостоятельно выбирает и использует цифровые средства общения, осуществляет поиск и/или создание контента в соответствии с целью взаимодействия, в том числе для организации совместной деятельности. | **Знать** цифровые средства общения с целью взаимодействия, в том числе для организации совместной деятельности.  **Уметь** самостоятельно выбирать и использовать цифровые средства общения, осуществлять поиск и/или создание контента в соответствии с целью взаимодействия, в том числе для организации совместной деятельности. | **Задание 1.** Разработайте политику информационной безопасности для системы идентификации физических лиц по биометрическим данным.  **Задание 2.** Для тестирования изменений и новых ИТ-технологий работники используют для тестирования данные, взятые из основной системы. Укажите нарушения ИБ, присвойте степень этим нарушениям, какие меры планируются для устранения этих нарушений, какие проетверки и сроки проверок. Обоснуйте ответ. |
| **Индикатор 2.** Владеет навыками организации взаимодействия и коммуникации с помощью информационных систем и/или цифровых сервисов и технологий. | **Знать**  способы организации взаимодействия и коммуникации с помощью информационных систем и/или цифровых сервисов и технологий.  **Уметь** организовывать взаимодействие и коммуникации с помощью информационных систем и/или цифровых сервисов и технологий, осуществлять подбор и применение различных информационно-коммуникационных средств для решения образовательных и профессиональных задач. | **Задача 1.** Вам необходимо защитить систему ведения счетов физических лиц от информационных угроз, связанных с реализацией DDos-атак. Составьте перечень мер по защите, приведите примеры специализированных средств защиты информации реализующих предложенные меры.  **Задача 2.** Разработайте модель угроз информационной безопасности для системы складского учета, доступ к которой осуществляется через внутренние выделенные каналы связи. |
|  | **Индикатор 3.**  Осуществляет подбор и применение различных информационно-коммуникационных средств для решения образовательных и профессиональных задач. | **Знать** информационно-коммуникационные средства для решения образовательных и профессиональных задач.  **Уметь** осуществлять подбор и применение различных информационно-коммуникационных средств для решения образовательных и профессиональных задач. | **Задача 1.** Разработайте методы и средства противодействия утечки информации для защиты системы обслуживания счетов юридических лиц, к которым сотрудники получают доступ через выделенную корпоративную сеть, а клиенты через выделенные каналы системы Банк-Клиент.  **Задача 2.** В компании необходимо организовать контрольно-пропускной режим, при условии а) доверенность считывания идентификаторов пользователей и б) высокая имитостойкость. Предложить методы идентификации и аутентификации с учетом условий. Назовите инструменты, отвечающих данным требованиям. |

**Примерный перечень вопросов к зачету**

* Определить сопровождаемость услуг, доступность услуг, надежность услуг.
* Информационные расчетные системы (системы операций по переводу денежных средств): назначение, функции, типовая архитектура, обрабатываемые данные, интерфейсы и системы взаимодействия, примеры продуктов. Обеспечение безопасности расчетных ИС (угрозы, уязвимости, методы и средства защиты).
* Системы ведения бухгалтерского учета: назначение, функции, типовая архитектура, обрабатываемые данные, интерфейсы и системы взаимодействия, примеры продуктов. Обеспечение безопасности ИС бухгалтерского учета (угрозы, уязвимости, методы и средства защиты).
* Статистические информационные системы: назначение, функции, типовая архитектура, обрабатываемые данные, интерфейсы и системы взаимодействия, примеры продуктов. Обеспечение безопасности статистических ИС (угрозы, уязвимости, методы и средства защиты).
* Информационные системы электронной коммерции: назначение, понятие электронной коммерции, операции электронной коммерции, функции, типовая архитектура, обрабатываемые данные, интерфейсы и системы взаимодействия, примеры продуктов. Обеспечение безопасности систем электронной коммерции (угрозы, уязвимости, методы и средства защиты).
* Информационные системы фондового рынка: назначение, операции фондового рынка, функции, типовая архитектура, обрабатываемые данные, интерфейсы и системы взаимодействия, примеры продуктов. Обеспечение безопасности систем фондового рынка(угрозы, уязвимости, методы и средства защиты).
* Информационные системы планирования: назначение, функции, типовая архитектура, обрабатываемые данные, интерфейсы и системы взаимодействия, примеры продуктов. Обеспечение безопасности систем планирования (угрозы, уязвимости, методы и средства защиты).
* Информационные системы управления персоналом (кадрами): назначение, функции, типовая архитектура, обрабатываемые данные, интерфейсы и системы взаимодействия, примеры продуктов. Обеспечение безопасности систем управления персоналом (угрозы, уязвимости, методы и средства защиты).
* Понятие недекларированные возможности ПО. Методы и инструменты выявления недекларированных возможностей ПО.
* Модель угроз безопасности ПО при разработке и внедрении.
* Этапы жизненного цикла ИС и их содержание.
* Базовые требования информационных систем персональных данных с учетом обеспечения требуемого уровня защищенности.
* Оценка качества ПО: показатели сопровождения ПО, показатели надежности, показатели доступности.
* Деятельность в рамках проектирования информационных систем.
* Перечислите деятельность, которая проводится на этапе Стратегического планирования ИС.
* Обеспечение безопасности процессов разработки программных продуктов методикой SDL.
* Политика ИБ. Перечислите содержание политики ИБ. Перечислите политики ИБ, которые рекомендуется разрабатывать в соответствии с международными стандартами ИСО/МЭК.
* Этапы Ввода системы в эксплуатацию и содержание работ каждого этапа. Назовите методы обеспечения безопасности на этапе Ввода системы.
* Деятельность и процессы этапа Эксплуатации ИС. Перечислите угрозы ПО на этапе эксплуатации и методы защиты.
* Практика динамического выделения инфраструктуры. Перечислите преимущества использования практики.
* Содержание этапа Совершенствования ИС.
* Определите суть практик Непрерывной интеграции, Непрерывной Поставки, Непрерывного развертывания.

**Примеры практико-ориентированных (ситуационных) заданий**

**Задача 1.** Определите уровень защищенности ИС, в которой обрабатываются данные: фио, возраст, форма лица, полученные от клиента.

**Задача 2**. Определите категорию ИС, в которой обрабатываются данные: фио, возраст, форма лица и вероисповедание субъекта, полученные из общедоступных источников.

**Задача 3.** В системе установлен парольный доступ, длина пароля равна 4 знакам, для пароля используются цифры от 0 до 9. Какое ограничение по количеству попыток необходимо ввести в систему, чтобы вероятность угадывания была не более 0,1?

**Задача 4.** Напишите базовые требования ИБ к модулю ведения счетов физических лиц с количеством клиентов меньше 10 000.

**Задача 5.** Разработайте требования по безопасности к модулю обработки платежей в рублях и иностранной валюте.

**Задача 6.** При проведении собеседования в HR-отделе компании сотрудник HR предлагает соискателю самостоятельно внести изменения в документы, используя для этого свободный компьютер, сообщает данные для входа в систему, после чего распечатывает измененные документы через сетевой принтер. Укажите на нарушения, присвойте степень этим нарушениям, какие меры планируются для устранения этих нарушений, определите каким образом следует проконтролировать устранение нарушений.

**Задача 7.** Программист работает над разработкой софта для клиента. При этом использует логический симулятор, который не был зарегистрирован у поставщика, на него отсутствует лицензия. Укажите на нарушения, присвойте степень этим нарушениям, какие меры планируются для устранения этих нарушений, какие проверки и в какие сроки должны быть проведены для контроля устранения нарушения.

**8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

**Рекомендуемая литература**

**Нормативные акты:**

1. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27000:2021 Информационные технологии. Системы менеджмента информационной безопасности.  
   Общий обзор и терминология. URL: <https://docs.cntd.ru/document/1200179675> (дата обращения: 02.04.2024). — Текст: электронный.
2. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27001:2005 Информационные технологии. Системы менеджмента информационной безопасности. Требования. URL: <https://docs.cntd.ru/document/1200181890> (дата обращения: 02.04.2024). — Текст: электронный.
3. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27002:2021 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью. URL: <https://docs.cntd.ru/document/1200179669> (дата обращения: 02.04.2024). — Текст: электронный.
4. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27003:2021 Информационные технологии. Системы менеджмента информационной безопасности. Руководство по реализации. URL: <https://docs.cntd.ru/document/1200179612> (дата обращения: 02.04.2024). — Текст: электронный.
5. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27004:2005 Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. URL: <https://docs.cntd.ru/document/1200179613> (дата обращения: 02.04.2024). — Текст: электронный.
6. Международный стандарт ISO/IEC 27005:2022 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности. URL: <https://cdn.standards.iteh.ai/samples/80585/7bca93ac16fd426a9bc717cadc9284d9/ISO-IEC-27005-2022.pdf> (дата обращения: 02.04.2024). — Текст: электронный.
7. Международный стандарт. ISO/IEC 27006:2020 Информационные технологии. Методы обеспечения безопасности. ТРЕБОВАНИЯ К ОРГАНАМ, ОСУЩЕСТВЛЯЮЩИМ АУДИТ И СЕРТИФИКАЦИЮ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. URL: <https://docs.cntd.ru/document/1200175373> (дата обращения: 02.04.2024). — Текст: электронный.
8. Международный стандарт. ISO/IEC 27007:2020 Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие указания по аудиту систем управления информационной безопасностью. URL: <https://www.iso.org/cms/%20render/live/ru/sites/isoorg/contents/data/standard/07/78/77802.html> (дата обращения: 02.04.2024). — Текст: электронный.
9. ГОСТ Р 57580.1-2017"Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер" URL: <https://docs.cntd.ru/document/1200146534> (дата обращения: 02.04.2024). — Текст: электронный.
10. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" URL: <https://base.garant.ru/70252506/> (дата обращения: 02.04.2024). — Текст: электронный.
11. ПРИКАЗ ФСТЭК. от 18 февраля 2013 г. N 21. ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> (дата обращения: 02.04.2024). — Текст: электронный.

**Рекомендуемая литература**

**а) основная:**

12.Гамза, В. А. Безопасность банковской деятельности : учебник для вузов / В. А. Гамза, И. Б. Ткачук, И. М. Жилкин. — 6-е изд., перераб. и доп. — Москва : Юрайт, 2024. — 455 с. — ЭБС Юрайт. - URL: https://urait.ru/bcode/531466 (дата обращения: 12.04.2024). – Текст : электронный.

13.Ларионова, С. Л. Информационная безопасность дистанционного банковского обслуживания: учебное пособие / С. Л. Ларионова; Финуниверситет. — Москва : Прометей, 2022. — 296 с. - Текст : непосредственный. - То же. - ЭБС Лань. - URL: https://e.lanbook.com/book/290516 (дата обращения: 12.04.2024). — Текст : электронный.

**б) дополнительная:**

|  |
| --- |
| 14. Жук, А. П. Защита информации : учеб. пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин [и др.]. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). - ЭБС ZNANIUM. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 12.04.2024). - Текст : электронный.  15. Зайцев, А. П. Технические средства и методы защиты информации: учебник для студентов вузов, обучающихся по группе специальностей - "Информационная безопасность" / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. – Москва : Горячая линия. - Телеком, 2019. - 442 с. – Текст : непосредственный. - То же. - 2012. - ЭБС ZNANIUM. - URL: http://znanium.com/catalog.php?bookinfo=390284 (дата обращения: 12.04.2024). - Текст : электронный. |

**9.** **Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**:

1. Сайт Центрального банка Российской Федерации: [www.cbr.ru](http://www.cbr.ru);
2. Сайт Федеральной службы по техническому и экспортному контролю: [www.fstec.ru](http://www.fstec.ru);
3. Сайт Федерального агентства по техническому регулированию и метрологии: [www.gost.ru](http://www.gost.ru).
4. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/
5. Электронно-библиотечная система BOOK.RU http://www.book.ru
6. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/
7. Электронно-библиотечная система издательства «ЮРАЙТ» https://urait.ru/
8. Электронно-библиотечная система издательства Лань https://e.lanbook.com/
9. Научная электронная библиотека eLibrary.ru http://elibrary.ru

# 10. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов реализуется в соответствии с приказом Финансового университета от 11.05.2021 № 1040/о «Об утверждении Методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете». Промежуточная аттестация проводится в соответствии с приказом Финансового университета от 23.03.2017 № 0557/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата и магистратуры в Финансовом университете». Кафедрой могут разрабатываться дополнительные методические рекомендации для отдельных форм проведения аудиторных занятий и самостоятельной работы студентов.

# 11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

**11.1. Комплект лицензионного программного обеспечения:**

Windows, Microsoft Office

Антивирус Kaspersky

**11.2 Современные профессиональные базы данных и информационные справочные системы:**

1. Информационно-правовая система «Гарант»

2. Информационно-правовая система «Консультант Плюс»

3. Электронная энциклопедия: http://ru.wikipedia.org/wiki/Wiki

4. Система комплексного раскрытия информации «СКРИН» -http://www.skrin.ru/11.3

**11.3 Сертифицированные программные и аппаратные средства защиты информации.**

Не используются.

# 12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Занятия по дисциплине проводятся в аудиториях, оборудованных мультимедийными комплексами, компьютерами с выходом в Интернет.