Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»

Кафедра аналитических и цифровых технологий

«УТВЕРЖДАЮ»
Проректор по учебно-
методической работе
_____Ю.А. Устименко
«30» июня 2022 г.

**Рабочая программа дисциплины**
**ФТД.01 Защита информации**

Направление подготовки 38.04.01 Экономика (уровень магистратуры)
Направленность (Профиль): Экономика и управление развитием организации
Форма обучения – заочная
Курс – 2
Семестр – 3
Всего зачетных единиц – 2, часов – 72
Форма отчетности: зачет – 3 семестр.

Программу разработал:
кандидат педагогических наук, доцент Д.А. Бояринов.

Одобрена на заседании кафедры аналитических и цифровых технологий
«23» июня 2022 г., протокол № 10

Заведующий кафедрой _____ Д.С. Букачев

Смоленск
2022

## 1. Место дисциплины в структуре ОП

Дисциплина «Защита информации» относится к факультативным дисциплинам направления подготовки 38.04.01 Экономика (уровень магистратуры).

Изучение дисциплины предполагает сочетание фундаментальной подготовки с освоением технологии применения специализированных программных продуктов и систем, ориентированных на защиту экономической и служебной информации, базируется на компетенциях, сформированных при изучении дисциплины «Информатика».

Сфера будущей деятельности связана, как правило, с необходимостью работы с информационными системами для хранения, обработки, передачи и защиты значительных объемов экономической и служебной информации, с необходимостью принимать управленческие решения и совершать юридические действия в точном соответствии с законом, поэтому изучение соответствующих информационных технологий и систем, а также нормативно-правовой базы для их грамотного использования в обязательном порядке входит в программу обучения студентов.

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

### 2. Планируемые результаты обучения по дисциплине

| Компетенция | Индикаторы достижения |
|---|---|
| **ПК-1.**<br>Способен определять приоритетные направления, подверженные рискам в организации, разрабатывать и оценивать ключевые индикаторы рисков, разрабатывать программы по управлению рисками при построении стратегий, управлять изменениями в организации, в т.ч. в условиях цифровой трансформации экономики | **Знать:** понятие риска и неопределенности, виды рисков, основы управления риском, правила анализа и оценки риска, методы оценки рисков и особенности их применения для разного вида рисков, основные способы снижения экономических рисков при построении стратегий, управлять изменениями в организации, в т.ч. в условиях цифровой трансформации экономики<br>**Уметь:** идентифицировать риск, осуществлять экспертную, статистическую и проектную оценку факторов риска, способных создавать социально-экономические ситуации критического характера, использовать закономерности и методы экономической науки при оценке риска, применять основные способы оценки и защиты от рисков при построении стратегий, управлять изменениями в организации, в т.ч. в условиях цифровой трансформации экономики<br>**Владеть:** методами экспертной, статистической и проектной оценки факторов риска, способных создавать социально-экономические ситуации критического характера, закономерностями и методами экономической науки при оценке риска, основными способами оценки и защиты от рисков при построении стратегий, управлять изменениями в организации, в т.ч. в условиях цифровой трансформации экономики |

## 3. Содержание дисциплины

**Тема 1. Обеспечение безопасности информационных систем.**

Способы и методы защиты информации. Защита от несанкционированного доступа. Особенности защиты информации в условиях современных сетевых технологий – проводных и беспроводных. Защита от вирусов. Сетевая безопасность. Электронная цифровая подпись: юридический и технический аспекты. Юридически значимый электронный документооборот.

**Тема 2. Основы компьютерной криптографии**

Использование защищенных компьютерных систем. Методы криптографии. Основные понятия криптографии. Открытый текст. Шифротекст. Криптографический алгоритм. Шифр Цезаря. Вскрытие шифра методом лобовой атаки. Понятие надежности криптографического алгоритма. Дополнительные задачи криптографического алгоритма - аутентификация источника сообщения, целостность, неотрицание авторства.

**Тема 3. Алгоритмы симметричного шифрования**

Шифрование с общим ключом. Проблема секретности общего ключа. Шифрование блоками и потоком. Раунды циклического алгоритма и подключи. Сеть Фейштеля. Дифференциальный и линейный криптоанализ. Алгоритм DES.

**Тема 4. Криптография с открытым ключом**

Алгоритмы шифрования с открытым ключом. Открытый и закрытый ключ. Алгоритм RSA. Алгоритм DSS. Обмен сессионных ключей. Виды криптосистем: симметричные криптосистемы, криптосистемы с открытым ключом, гибридные криптосистемы.

**Тема 5. Хеш-функции и аутентификация сообщений. Цифровая подпись. Цифровой сертификат**

Закон РФ «Об электронной цифровой подписи». Требования к хеш-функциям. Простые и сложные хеш-функции. Хеш-функция MD-5. Хеш-функция SHA-1. Цифровая подпись. Прямая и арбитражная цифровые подписи. Стандарт цифровой подписи DSS. Цифровые сертификаты. Доверительные центры.

**Тема 6. Построение защищенных информационных систем**

Основные технологии построения защищённых информационных систем. Оценки стоимости проведения мероприятий по безопасности. Вопросы разработки и реализации политики безопасности. Управление доступом. Аудит систем. Системы отчетности по безопасности. Сканирование уязвимых мест информационных систем. Место информационной безопасности информационных систем в национальной безопасности страны.

## 4. Тематический план

| № п/п | Разделы и темы | Всего часов | Формы занятий | | | |
|---|---|---|---|---|---|---|
| | | | Лекции | Практич. занятия | Лаборатор. занятия | Самостоя-тельная работа |
| 1. | Обеспечение безопасности информационных систем. | 12 | 0 | 0 | 0 | 12 |
| 2. | Основы компьютерной криптографии | 12 | 0 | 0 | 0 | 12 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3. | Алгоритмы симметричного шифрования | 12 | 0 | 0 | 0 | 12 |
| 4. | Криптография с открытым ключом | 12 | 0 | 0 | 0 | 12 |
| 5. | Хеш-функции и аутентификация сообщений. Цифровая подпись. Цифровой сертификат | 12 | 0 | 0 | 0 | 12 |
| 6. | Построение защищенных информационных систем | 12 | 0 | 0 | 0 | 12 |
| Всего за семестр | | 72 | 0 | 0 | 0 | 72 |

## 5. Виды учебной деятельности

**Лекции** не предусмотрены.

**Лабораторные занятия** не предусмотрены.

**Практические занятия** не предусмотрены.

**Самостоятельная работа**

Самостоятельная работа студентов направлена на углубление и закрепление знаний, а также развитие практических умений и заключается в:

- поиске и анализе литературы и электронных источников информации;
- выполнении домашних заданий для самостоятельного выполнения.

### Задания для самостоятельного выполнения

1. Настроить сетевой экран АРМ по принципу «белого списка». Обосновать необходимость созданных правил сетевого экрана.
2. Расшифровать шифротекст с использованием результатов проведенного частотного анализа.
3. Осуществить дешифрование трафика, зашифрованного симметрическим способом.
4. Осуществить дешифрование трафика, зашифрованного асимметрическим способом.
5. Расшифровать зашифрованный симметрическим способом документ от преподавателя.
6. Расшифровать зашифрованный асимметрическим способом документ от преподавателя.
7. Сгенерировать хеш SHA-1 для исходного и модифицированного файла, сравнить хеши.
8. Осуществить проверку контрагентов организации на благонадежность в Контур.Фокус.
9. Осуществить настройку и реализовать формализованный и неформализованный электронный документооборот с ПФР и Росстатом на базе Контур.Экстерн.

### Вопросы для самостоятельного изучения

**Вопросы для самостоятельного изучения темы 1**

1. Признаки классификации систем электронного документооборота.
2. Различие технологий workflow и docflow.

3. Особенности конфиденциального электронного документооборота.

4. Основные виды защищаемой информации в системе электронного документооборота, виды документов ограниченного доступа.

5. Уровни конфиденциальности информации, обрабатываемые в системах электронного документооборота.

6. Угрозы безопасности информации в системах электронного документооборота.

7. Защита от вредоносных программ систем электронного документооборота.

8. Особенности аппаратной защиты электронного обмена информацией.

9. Особенности резидентного компонента безопасности.

10. Принципы аппаратной реализации механизмов аутентификации в электронной среде.

11. Интерфейсные средства электронного обмена информацией.

12. Техническая реализация аппаратных средств защиты информации.

13. Система контроля целостности и подтверждения достоверности электронных документов. Применение кодов аутентификации в подсистемах технологической защиты информации.

14. Эффективность аппаратных средств защиты.

15. Организация электронного почтового взаимодействия.

16. Роль и функции электронной почты.

17. Основные принципы организации электронной почты.

18. Угрозы безопасности информации, связанные с использованием электронной почты.

**Вопросы для самостоятельного изучения темы 2**

1. Традиционные методы шифрования (подстановки, перестановки, замены + пример)
2. Понятие одноразового блокнота и шифр гаммирования
3. Метод умножения Карацубы.
4. Решение диофантовых уравнений 1-й степени.
5. Криптосистемы без передачи ключей (достоинства, недостатки)

**Вопросы для самостоятельного изучения темы 3**

1. Классификация криптосистем.
2. Алгоритм DES. Область применения DES.
3. Блочные и поточные шифры.
4. Отечественный стандарт шифрования.
5. Псевдослучайная последовательность и ее применение в криптографии.

**Вопросы для самостоятельного изучения темы 4**

1. Дискретный логарифм. Вычисление дискретного логарифма
2. Процедура шифрования и расшифрования в криптосистемах RSA
3. Безопасность и быстродействие RSA.
4. Отечественные стандарты асимметричного шифрования.
5. Комбинированный метод шифрования
6. Защита платежных (банковских) систем.

**Вопросы для самостоятельного изучения темы 5**

1. Аутентификация пользователя и сообщения.

2. Криптостойкие хеш-функции. Хеш-значение.
3. Взломостойкость современных хеш-функций.
4. Коллизии и методы борьбы с ними.
5. Хеширование и электронная подпись.
6. Механизм работы удостоверяющего центра.

**Вопросы для самостоятельного изучения темы 6**

1. Оценка защищенности систем ЭДО.
2. Технический аспект безопасности систем ЭДО.
3. Задачи и полномочия системного администратора.
4. Механизмы управления доступом в системах ЭДО.

Критерии оценивания ответов на вопросы для самостоятельного изучения

Ответ по каждому вопросу оценивается по пятибалльной шкале в зависимости от содержательности ответа и логики изложения материала.

## Оценочные средства

### 6.1. Оценочные средства и критерии оценивания для текущей аттестации

**Задания для самостоятельного выполнения**

Критерии оценивания заданий для самостоятельного выполнения.

| Уровень выполнения | Оценка |
|---|---|
| Задача решена в полном объёме, алгоритмические и вычислительные ошибки отсутствуют, проведен анализ полученного решения. | 5 (отлично) |
| Задача решена в полном объёме с незначительными техническими ошибками или отсутствует анализ результатов решения. | 4 (хорошо) |
| Задача решена не полностью или в решении присутствуют ошибки алгоритмического характера, незначительно влияющие на ход решения. | 3 (удовлетворительно) |
| Задача не решена или в решении присутствует значительное количество ошибок алгоритмического характера, существенно влияющих на ход решения. | 2 (неудовлетворительно) |

**Вопросы для самостоятельного изучения**

Критерии оценивания ответов на вопросы для самостоятельного изучения

Ответ по каждому вопросу оценивается по пятибалльной шкале в зависимости от содержательности ответа и логики изложения материала.

| Уровень ответа | Оценка |
|---|---|
| Полно и аргументировано отвечает по содержанию темы; может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из лекции, но и самостоятельно составленные; излагает материал последовательно и корректно. | 5 (отлично) |
| Дает ответ, удовлетворяющий тем же требованиям, что и для оценки «5», но допускает 1-2 ошибки, которые сам же исправляет. | 4 (хорошо) |
| Излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки. | 3 (удовлетворительно) |
| Не знает ответ на вопрос, допускает существенные ошибки в формулировке определений и алгоритмов, искажающие их смысл, беспорядочно и неуверенно излагает материал. | 2 (неудовлетворительно) |

### 6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

**Критерии получения зачета**

Зачет выставляется по результатам работы студента в течение семестра согласно Положению о текущем контроле успеваемости и промежуточной аттестации студентов в

федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Смоленский государственный университет».

Для получения зачета студент должен:

- выполнить задания для самостоятельной работы на оценку не ниже «удовлетворительно»;
- уметь отвечать на вопросы для самостоятельного изучения и вопросы по теоретической части курса на оценку не ниже «удовлетворительно».

### 7.1. Основная литература


1. *Зенков, А. В.* Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002
2. *Суворова, Г. М.* Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741
3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844


### 7.2. Дополнительная литература


1. *Корабельников, С. М.* Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496492
2. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489745
3. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490421

### 7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Свободно доступные курсы Интернет-университета информационных технологий (ИНТУИТ) http://www.intuit.ru/;
2. Портал государственных и муниципальных услуг. http://www.gosuslugi.ru/;
3. Официальный сайт ЗАО «Консультант Плюс» – www.consultant.ru;
4. Официальный сайт ООО «НПП Гарант-Сервис» – www.garant.ru;
5. www.compress.ru – Сайт журнала «КомпьютерПресс».

### 7.4 Методические указания для обучающихся по освоению дисциплины

1. Методические указания к выполнению лабораторных работ компании СКБ «Контур» курса для студентов. URL: https://school.kontur.ru/courses/ap-2.

## 8. Материально-техническое обеспечение

**Учебная аудитория для проведения занятий лекционного типа**. Аудитория 124 уч.к. № 2.
Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.
Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 18 шт., колонки Genius – 18 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.
Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).
**Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – компьютерный класс.** Аудитория 124 уч.к. №2.
Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.
Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 16 шт., колонки Genius – 16 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.
Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).
**Помещение для самостоятельной работы – компьютерный класс с доступом к сети «Интернет» и ЭИОС СмолГУ**. Аудитория 124 уч.к. №2.
Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.
Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 18 шт., колонки Genius – 18 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.
Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).

## 9. Программное обеспечение

1.Kaspersky Endpoint Security для бизнеса Стандартный АО «Лаборатория Касперского».
2. Microsoft Open License в составе:
– Microsoft Windows Professional XP, 7, 8 Server Russian;
– Microsoft Office 2003-2016 Russian.
3. СКЗИ КриптоПро (лицензия, интегрированная в сертификат для образовательных курсов в рамках программы академического партнерства с СКБ Контур).
4. Веб-сервисы безбумажного юридически значимого документооборота компании СКБ «Контур» (в рамках программы академического партнерства с СКБ Контур).
5. Конфигурации на базе 1С: Предприятие 8.3.
6. BackTrack 5 R3 (свободно распространяемая сборка ПО на базе Linux для системного администрирования, URL:http://nextleveltricks.com).

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

**Сертификат:** 6314D932A1EC8352F4BBFDEFD0AA3F30
**Владелец: Артеменков Михаил Николаевич**
**Действителен:** с 21.09.2022 до 15.12.2023