МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

Защита электронного документооборта

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план b090302_25_BIS25.plx
09.03.02 Информационные системы и технологии

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 0
в том числе:
аудиторные занятия 0
самостоятельная работа 0

Виды контроля в семестрах:

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	28	32	28
Практические	32	28	32	28
Иные виды контактной работы	0,25	0,25	0,25	0,25
Итого ауд.	64,25	56,25	64,25	56,25
Контактная работа	64,25	56,25	64,25	56,25
Сам. работа	43,75	51,75	43,75	51,75
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины «Защита электронного документооборота» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации в системах электронного документооборота, анализом возможных угроз в информационной сфере и адекватных мер по их нейтрализации, а также содействие фундаментализации образования и развитию системного мышления.
1.2	Задачи дисциплины:
1.3	• исследование моделей электронного документооборота критически важных объектов;
1.4	• разработка модели угроз и модели нарушителя защищенной системы электронного документооборота критически важных объектов;
1.5	• разработка защищенных систем электронного документооборота критически важных объектов;
1.6	• проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации ;
1.7	• разработка технических регламентов, проектов нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов по защите систем электронного документооборота.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Автоматизированные системы управления
2.1.2	Современные киберугрозы в промышленных и корпоративных системах автоматизации
2.1.3	Мониторинг информационной безопасности автоматизированных систем управления
2.1.4	Инженерно-техническая защита информации и технические средства охраны
2.1.5	Практикум по решению эксплуатационных задач профессиональной деятельности
2.1.6	Цифровая обработка сигналов в системах обеспечения информационной безопасности автоматизированных систем управления
2.1.7	Методы и средства противодействия террористической деятельности в системах управления значимых объектов КИИ
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-3.3: Способен проводить тестирование ПО по разработанным тестовым случаям
Знать:
Уметь:
Владеть:

ПК-4.3: Способен проводить мониторинг работы БД
Знать:
Уметь:
Владеть:

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями в безопасности SIEM;
3.1.2	принципы работы систем мониторинга информационной безопасности автоматизированных систем;
3.1.3	актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности, типы современных киберугроз в промышленных и
3.1.4	корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;
3.1.5	средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации;
3.1.6	цели и задачи проектирования систем инженерно-технической защиты объектов;

3.1.7	основные понятия и терминологию, принятые в проектировании систем инженерно-технической защиты объектов;
3.1.8	основные принципы проектирования систем инженерно-технической защиты объектов, физические принципы, на которых строятся системы;
3.1.9	цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ;
3.1.10	состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления, архитектуру промышленных сетей АСУ ТП инженерно-технической защиты объектов.
3.2	**Уметь:**
3.2.1	использовать средства сбора и анализа информации о событиях информационной безопасности для целей мониторинга информационной безопасности;формировать правила анализа событий мониторинга информационной безопасности автоматизированных систем;
3.2.2	анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации, проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;
3.2.3	проводить анализ вероятных угроз охраняемому объекту;выбирать наиболее рациональные методы противодействия угрозам
3.2.4	охраняемому объекту;
3.2.5	выбирать технические средства для решения задачи охраны объекта, проводить оптимизацию структуры комплексов инженерно- технической защиты объектов;
3.2.6	анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации, применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП
3.3	**Владеть:**
3.3.1	использования методов мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;
3.3.2	идентификации и моделирования каналов возможного деструктивного информационно-технического воздействия в промышленных и
3.3.3	корпоративных системах автоматизации, оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП;
3.3.4	анализа критериев оценки параметров технических средств охраны объектов;составления программы испытаний систем инженерно-технической защиты объектов;
3.3.5	определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Введение						
1.1	Введение /Лек/	7	2		Л1.1 Л1.2Л2.1	0	
1.2	Выполнение домашней работы /Ср/	7	13		Л1.1 Л1.2Л2.1	0	
	Раздел 2. Понятие «электронный документ», «электронный документооборот»						
2.1	Понятие «электронный документ», «электронный документооборот» /Пр/	7	4		Л1.1 Л1.2Л2.1	0	
2.2	Понятие «электронный документ», «электронный документооборот» /Лек/	7	4		Л1.1 Л1.2Л2.1	0	
2.3	Написание реферата /Ср/	7	5		Л1.1 Л1.2Л2.1	0	
	Раздел 3. Нормативная правовая база в сфере электронного документооборота						
3.1	Нормативная правовая база в сфере электронного документооборота /Лек/	7	4		Л1.1 Л1.2Л2.1	0	
3.2	Нормативная правовая база в сфере электронного документооборота /Пр/	7	4		Л1.1 Л1.2Л2.1	0	

3.3	Подготовка доклада /Ср/	7	6		Л1.1 Л1.2Л2.1	0	
	Раздел 4. Классификация систем электронного документооборота						
4.1	Классификация систем электронного документооборота /Лек/	7	6		Л1.1 Л1.2Л2.1	0	
4.2	Классификация систем электронного документооборота /Пр/	7	6		Л1.1 Л1.2Л2.1	0	
	Раздел 5. Основные функции систем электронного документооборота						
5.1	Основные функции систем электронного документооборота /Лек/	7	4		Л1.1 Л1.2Л2.1	0	
5.2	Основные функции систем электронного документооборота /Пр/	7	6		Л1.1 Л1.2Л2.1	0	
5.3	Изучение и конспектирование документов /Ср/	7	5,75		Л1.1 Л1.2Л2.1	0	
5.4	Самостоятельное изучение темы /Ср/	7	8		Л1.1 Л1.2Л2.1	0	
	Раздел 6. Идентификация, аутентификация, авторизация в системе электронного документооборота						
6.1	Идентификация, аутентификация, авторизация в системе электронного документооборота /Лек/	7	6		Л1.1 Л1.2Л2.1	0	
6.2	Разграничение прав пользователей в системе электронного документооборота. Матрица доступа /Пр/	7	4		Л1.1 Л1.2Л2.1	0	
	Раздел 7. Электронные подписи						
7.1	Электронные подписи /Лек/	7	2		Л1.1 Л1.2Л2.1	0	
7.2	Электронные подписи /Пр/	7	4		Л1.1 Л1.2Л2.1	0	
7.3	Подготовка к зачету /Ср/	7	14		Л1.1 Л1.2Л2.1	0	
7.4	Зачет /ИВКР/	7	0,25		Л1.1 Л1.2Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Введение
1. Что такое электронный документооборот и каково его значение в современных организациях?
2. Какие задачи решает внедрение систем электронного документооборота (СЭД)?
3. Какова роль электронного документооборота в цифровизации бизнес-процессов?
4. Какие преимущества даёт переход от бумажного к электронному документообороту?
5. Какие ключевые тенденции развития электронного документооборота в России и за рубежом?
Тема 2: Понятие «электронный документ», «электронный документооборот»
6. Что понимается под электронным документом?
7. Чем отличается электронный документ от бумажного аналога?
8. Что такое электронный документооборот и какие этапы он включает?
9. Какие виды документов чаще всего переводятся в электронный формат?
10. Как обеспечивается юридическая значимость электронных документов?
Тема 3: Нормативная правовая база в сфере электронного документооборота
11. Какие законы регулируют использование электронных документов в РФ?
12. Каково значение ФЗ №63 "Об электронной подписи"?
13. Какие требования предъявляет законодательство к хранению электронных документов?
14. Какие положения Гражданского кодекса РФ относятся к электронному документообороту?
15. Как осуществляется сертификация и аккредитация удостоверяющих центров?
Тема 4: Классификация систем электронного документооборота
16. Как классифицируются системы электронного документооборота?
17. Чем отличаются корпоративные и межорганизационные СЭД?
18. Какие СЭД используются в государственных органах?

19. Какие платформы и решения наиболее популярны на российском рынке СЭД?
20. Какие факторы влияют на выбор системы электронного документооборота?
Тема 5: Основные функции систем электронного документооборота
21. Какие основные модули входят в состав типовой СЭД?
22. Как организуется маршрутизация документов внутри системы?
23. Как реализуется поиск и фильтрация документов в СЭД?
24. Какие инструменты используются для работы с задачами и поручениями?
25. Как интегрируются СЭД с ERP, CRM и другими информационными системами?
Тема 6: Идентификация, аутентификация, авторизация в СЭД
26. Что такое идентификация и аутентификация в системах документооборота?
27. Какие методы аутентификации поддерживаются в СЭД?
28. Как реализуется двухфакторная аутентификация?
29. Как происходит учёт действий пользователей в системе?
30. Как обеспечивается защита от несанкционированного доступа к документам?
Тема 7: Разграничение прав пользователей в СЭД. Матрица доступа
31. Что такое разграничение прав доступа в СЭД?
32. Какие уровни доступа к документам обычно реализуются?
33. Что такое матрица доступа и как она используется?
34. Как организуется работа с ролями и группами пользователей?
35. Какие политики безопасности применяются при управлении доступом?
Тема 8: Электронные подписи
36. Что такое электронная подпись и какие виды существуют?
37. Чем отличаются простая, усиленная квалифицированная электронные подписи?
38. Как работает алгоритм создания и проверки электронной подписи?
39. Какие требования предъявляются к Удостоверяющим центрам?
40. Как использовать электронную подпись в государственных и коммерческих системах?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Защита электронного документооборта" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 11 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Ковалева Н. Н., Жирнова Н. А., Тугушева Ю. М., Холодная Е. В.	Информационное право. Практикум: учебное пособие для вузов	Москва: Юрайт, 2024
Л1.2	Краковский Ю. М.	Методы и средства защиты информации: учебное пособие для вузов	Санкт-Петербург: Лань, 2025

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Ковалева Н. Н., Брянцев И. И., Брянцева О. В., Варламова Е. В., Ересько П. В., Жирнова Н. А., Изотова В. Ф., Ильгова Е. В., Сергеева Е. Ю., Солдаткина О. Л., Тугушева Ю. М., Холодная Е. В., Чайковский Д. С.	Информационное право: учебник для вузов	Москва: Юрайт, 2024
6.3.1 Перечень программного обеспечения			
6.3.1.1	Office Professional Plus 2019		
6.3.1.2	Windows 10		
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.	
6.3.2 Перечень информационных справочных систем			
6.3.2.1	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")		
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"		
6.3.2.3	База данных научных электронных журналов "eLibrary"		

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

6-25	Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для организации практической подготовки обучающихся	Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор; Экран; ПК с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Телекоммуникационные шкафы; Средства отображения информации. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов в составе: Учебный стенд "Основы IP-сетей" (маршрутизаторы, коммутаторы L2/L3); Учебный стенд "Виртуальные сети (VLAN, VPN)"; Учебный стенд "Беспроводные сети (Wi-Fi, IoT)"; Учебный стенд "Телефония (ISDN, VoIP)"; Учебный стенд "Оптические сети (PON, DWDM)"; Стенд "Цифровые системы передачи (E1, SDH)". Стенды для изучения проводных и беспроводных компьютерных сетей в составе: абонентские устройства; коммутаторы; маршрутизаторы; точкидоступа, межсетевые экраны; средства обнаружения компьютерных атак; системы углубленной проверки сетевых пакетов; системы защиты от утечки данных; анализаторы кабельных сетей. Учебно-лабораторные комплексы в составе: Учебный лабораторный комплекс контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры). Учебный лабораторный комплекс проведения анализа защищенности значимого объекта КИИ на соответствие	

		требованиям по обеспечению безопасности. Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе: средства защиты информации от НСД; программно-аппаратный комплекс доверенной нагрузки; антивирусные программные комплексы; межсетевые экраны; средства создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса; программа поиска и гарантированного уничтожения информации на дисках; аппаратные средства аутентификации пользователя; системы обнаружения вторжений и анализа защищенности; средства анализа защищенности компьютерных сетей; сканеры безопасности; устройства чтения смарт-карт и радиометок; программно-аппаратные комплексы защиты информации; средства криптографической защиты информации. Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД. Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД. УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации. Аппаратно-программные комплексы в составе: аппаратно-программные средства управления	

		доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем; средства контроля и управления доступом в помещения.	
5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Защита электронного документооборта" представлены в Приложении 2 и включают в себя:
1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.