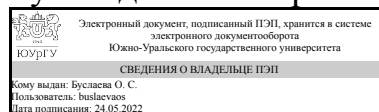


УТВЕРЖДАЮ:
Руководитель направления



О. С. Буслаева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.01 Защита информации в корпоративных информационных системах

для направления 09.04.02 Информационные системы и технологии

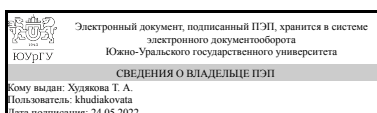
уровень Магистратура

форма обучения очная

кафедра-разработчик Цифровая экономика и информационные технологии

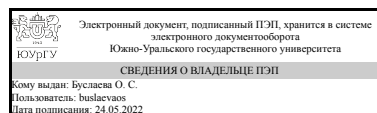
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.04.02 Информационные системы и технологии, утверждённым приказом Минобрнауки от 19.09.2017 № 917

Зав.кафедрой разработчика,
Д.ЭКОН.Н., доц.



Т. А. Худякова

Разработчик программы,
к.техн.н., доцент



О. С. Буслаева

1. Цели и задачи дисциплины

Цель изучения дисциплины - получить базовые знания в области защиты информации в корпоративных информационных системах (КИС). Задачи изучения дисциплины: • освоение методов защиты рабочих станций и серверов, входящих в состав КИС; • получение навыков проектирования, внедрения и сопровождения эксплуатации защищенных каналов передачи информации в распределенных корпоративных информационных системах.

Краткое содержание дисциплины

Защищенность информационной среды организации и ее составной части КИС — одно из основных условий ее эффективного функционирования. Комплекс мероприятий по обеспечению информационной безопасности КИС должен быть неотъемлемой частью системы управления любой организации. Дисциплина обеспечивает знакомство студента с теоретическими основами криптографии, инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения КИС, практическими приемами защиты рабочих станций и серверов, составляющих КИС.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-3 Способен разрабатывать требования к программным продуктам и программному обеспечению, отслеживать системность и качество работы программистов	Знает: потенциальные угрозы безопасности КИС; основные правила обеспечения безопасности рабочих станций и серверов, входящих в состав КИС; роль разработчика в построении безопасных приложений для КИС; принципиальные положения норм международного права в области авторских и смежных прав, патентного права; - содержание норм российского права в области авторских и смежных прав, патентного права; методы оценки качества Умеет: исследовать проблемы при реализации систем безопасности КИС; настраивать почтовые сервисы (в составе КИС) для обеспечения конфиденциальности электронной переписки; обеспечивать конфиденциальность и аутентичность при взаимодействии приложений, входящих в состав программного обеспечения КИС; квалифицированно пользоваться международными документами и национального законодательства в сфере авторских и смежных прав, патентного права; оценивать угрозы информационной безопасности; определять объекты учета и оценивать затраты ИТ; рассчитывать стоимость сервиса ИТ на основе функционально- стоимостного анализа; Имеет практический опыт: использования программных средств реализации сервисов

конфиденциальности, целостности, аутентичности для КИС; использования информационно-правовых систем,

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	ФД.02 Защита интеллектуальной собственности

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Нет

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 74,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		1	
Общая трудоёмкость дисциплины	144	144	
<i>Аудиторные занятия:</i>	64	64	
Лекции (Л)	32	32	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>	69,5	69,5	
с применением дистанционных образовательных технологий	0		
Подготовка к экзамену	27	27	
Подготовка к выполнению практических заданий № 1-23	42,5	42,5	
Консультации и промежуточная аттестация	10,5	10,5	
Вид контроля (зачет, диф.зачет, экзамен)	-	экзамен	

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основные понятия и термины, относящиеся к информационной безопасности. Характерные проблемы, связанные с безопасностью, при использовании компьютерных сетей. Классификация атак. Сервисы безопасности. Правила обеспечения безопасности рабочей	16	8	8	0

	станции.				
2	Криптография симметричная и асимметричная (с открытым ключом). Основные понятия и термины. Факторы безопасности алгоритмов шифрования, хэширования, цифровой подписи. Примеры алгоритмов их программная реализация (на примере open source) Gpg, Pgp (Pgp sdk), Openssl, TrueCrypt.	20	12	8	0
3	Криптографические стандарты КИС. Цифровые сертификаты. Иерархия центров авторизации. Серверные и клиентские сертификаты. Безопасные коммуникации.	16	8	8	0
4	Советы и рекомендации. Практика разработки систем безопасности КИС. Методы безопасного кодирования. Полезные ресурсы.	12	4	8	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1-3	1	Характерные проблемы, связанные с безопасностью, при использовании КИС. Последствия слабой системы безопасности КИС. Проблемы при реализации системы безопасности КИС. Роль разработчика в построении безопасных приложений для КИС. Классификация атак на сервисы безопасности КИС. Правила обеспечения безопасности рабочих станций и серверов КИС. Выполнение обновлений операционных систем КИС. Выполнение обновлений прикладных программ КИС. Установка антивирусной программы и регулярное обновление антивирусных баз. Настройка брандмауэров сетевого периметра КИС. Построение демилитаризованной зоны КИС. Настройка персональных бранд-мауэров рабочих станций и серверов в составе КИС. Администрирование КИС под учетной записью пользователя с минимальным необходимым уровнем привилегий. Аудит защищаемых ресурсов КИС. «Физическая» защита рабочих станций и серверов КИС. Шифрование конфиденциальной информации КИС. Архивация данных КИС. Тренинг персонала (противодействие социальной инженерии ...). План восстановительных операций КИС.	6
4	1	Практика разработки систем безопасности КИС. Методы безопасного кодирования. Полезные ресурсы.	2
5-7	2	Криптография. Криптоанализ. Стеганография. Факторы безопасности алгоритмов симметричного шифрования. Абсолютно стойкий шифр. Алгоритмы ГОСТ 28147-89, AES. Режимы симметричного блочного шифрования длинных сообщений. Основные требования к алгоритмам асимметричного шифрования (шифрования с открытым ключом). Понятие односторонней функции с секретом. Правила модульной арифметики.	6
8-10	2	Способы использования алгоритмов с открытым ключом (зашифрование/расшифрование). Цифровая подпись (прямая, арбитражная). Алгоритм RSA, схема Диффи-Хеллмана, стандарт цифровой подписи DSS. Отечественные стандарты алгоритмов с открытым ключом. Криптографические хэш-функции. Основные требования. Отечественные и зарубежные стандарты.	6
11-13	3	Криптографические стандарты КИС. Спецификации PKI. Серверные и клиентские цифровые сертификаты. Безопасные коммуникации на основе TLS/SSL.	6
14	3	Спец. главы	2
15-16	4	Спец. главы	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Оценка уязвимостей КИС (на примере Nessus, nmap)	2
2	1	Настройка обновлений ОС рабочих станций и серверов КИС (на примере WSUS).	2
3	1	Разграничение доступа и обеспечение конфиденциальности данных КИС, хранящихся на встроенных и съемных носителях информации (на примере EFS, GPG, TrueCrypt).	2
4	1	Проектирование демилитаризованной зоны (ДМЗ) для защиты периметра КИС от внутренних и внешних сетевых угроз.	2
5	2	Разграничение доступа и обеспечение конфиденциальности данных КИС, хранящихся на встроенных и съемных носителях информации (на примере EFS, GPG, TrueCrypt).	2
6-7	2	Защита почтовых протоколов, используемых КИС: • настройка защищенного почтового канала (Putty+sshd) • настройка защищенного почтового канала (stunnel) • разработка приложения для защищенного приема электронной почты по протоколу POP3 (TLS/SSL) • разработка приложения для защищенной передачи электронной почты по протоколу Smtп (TLS/SSL)	4
8	2	Разработка правил внутреннего и внешнего фаерволов ДМЗ (на примере фаервола IPFW для FreeBSD).	2
9-11	3	Использование GPG для обеспечения конфиденциальности содержания электронной почты; Использование Public Key Infrastructure (PKI) для обеспечения конфиденциальности содержания электронной почты.	6
12	3	Настройка удаленного доступа к ресурсам КИС.	2
13	4	Защита баз данных и web-приложений КИС.	2
14-15	4	Разработка систем защищенного лицензирования ПО КИС.	4
16	4	Аудит защищенности КИС на основе криптоанализа хранящихся данных.	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к экзамену	Малюк, А.А. Введение в информационную безопасность. [Электронный ресурс] / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 288 с.; Бирюков, А.А. Информационная безопасность: защита и нападение. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2012. — 474 с.	1	27
Подготовка к выполнению практических заданий № 1-23	Суховилов, Б. М. Защита информации в корпоративных информационных системах Текст учеб. пособие к практ.	1	42,5

	работам по направлению "Приклад. информатика" Б. М. Суховилов ; Юж.-Урал. гос. ун-т, Каф. Информатика ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2013. - 39, [1] с. ил. электрон. версия		
--	---	--	--

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учитывается в ПА
1	1	Промежуточная аттестация	Экзамен	-	15	Экзамен проводится в устной форме. Каждому студенту выдается билет с 3 вопросами. Время на подготовку отводится 30 минут. За каждый вопрос выставляется баллы. Максимальный балл за вопрос - 5. 5 баллов - Грамотный полный (развернутый) ответ на теоретический вопрос; 4 балла - дан правильный, но краткий ответ на вопрос; 3 балла - дан в общем правильный ответ на вопрос, но с замечаниями; 2 балла - дан неполный ответ на вопрос, но на уточняющие вопросы отвечено; 1 балл - дан неправильный ответ на вопрос, но на уточняющие вопросы даны правильные ответы; 0 -баллов - ответ на вопрос не дан	экзамен
2	1	Текущий контроль	Выполнение практических работ	1	20	В процессе обучения студент выполняет практические задания и затем защищает их. Всего предлагается выполнить 4 практических заданий. Каждая практическая работа оценивается в 5 баллов. 5 баллов - студент выполнил правильно работу, ответил на вопросы; 4 балла - правильно выполнен работу, ответил не на все вопросы; 3 балла - есть замечания по самостоятельным работам, но во время защиты ошибки были исправлены; 2 балла - выполнена самостоятельная работа с ошибками, не на все вопросы даны правильные ответы; 1 балл - работы сделаны с ошибками, сданы после срока; 0 баллов - срок сдачи превысил 2 занятия	экзамен

3	1	Текущий контроль	Тестирование №1	1	20	Тест состоит из 20 вопросов, позволяющих оценить сформированность компетенций. На ответы отводится 10 минут. Правильный ответ на вопрос соответствует 1 баллу. Неправильный ответ на вопрос соответствует 0 баллов.	экзамен
4	1	Текущий контроль	Защита доклада	1	8	Для подготовки к докладу студентам выдаются темы для самостоятельного изучения. Доклад по теме готовится индивидуально. Защита доклада сопровождается презентацией, ответами на вопросы. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: - содержание: 2 балла – содержание полностью соответствует теме доклада, тема раскрыта полностью; 1 балл – содержание доклада не полностью соответствует теме и/или раскрыты не все аспекты темы; 0 баллов – содержание доклада не соответствует теме. - оформление: 2 балла – презентация оформлена в соответствии с выданным заданием; 1 балл – в презентации выявлены недочеты; 0 баллов – студент неверно оформил презентацию или не выполнил задание. - срочность: 2 балла – доклад защищен в назначенный срок; 1 балл – доклад защищен на следующем занятии или консультации, после назначенного срока; 0 баллов – доклад защищен позднее, чем на следующем занятии или консультации. Ответы на вопросы: 2 балла – студент дает развернутые ответы на вопросы; 1 балл – студент дает краткий ответ, либо отвечает с уточняющими вопросами; 0 баллов – студент не может ответить на вопросы.	экзамен
5	1	Текущий контроль	Тестирование №2	1	20	Тест состоит из 20 вопросов, позволяющих оценить сформированность компетенций. На ответы отводится 10 минут. Правильный ответ на вопрос соответствует 1 баллу. Неправильный ответ на вопрос соответствует 0 баллов.	экзамен

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	При оценивании результатов учебной деятельности	В соответствии

	<p>обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (Положение о БРС утверждено приказом ректора от 24.05.2019 г. № 179, в редакции приказа ректора от 10.03.2022 г. № 25-13/09). Оценка за дисциплину формируется на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. Отлично: величина рейтинга обучающегося по дисциплине 85...100 %. Хорошо: величина рейтинга обучающегося по дисциплине 75...84 %. Удовлетворительно: величина рейтинга обучающегося по дисциплине 60...74 %. Неудовлетворительно: величина рейтинга обучающегося по дисциплине 0...59 %.</p> <p>Если студент не согласен с оценкой, полученной по результатам текущего контроля, студент проходит мероприятие промежуточной аттестации. Промежуточная аттестация проводится устно по билетам. Каждый билет содержит 3 вопроса, позволяющих оценить сформированность компетенций. На подготовку дается 30 минут, после чего студент отвечает на вопросы в билете. Для уточнения уровня знаний студента преподаватель может задать от одного до трех дополнительных вопросов по темам курса. В случае прохождения мероприятия промежуточной аттестации оценка за дисциплину рассчитывается на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. Фиксация результатов учебной деятельности по дисциплине проводится в день проведения экзамена при личном присутствии студента. Оценка по дисциплине вносится в «Приложение к диплому магистра»</p>	с пп. 2.5, 2.6 Положения
--	--	--------------------------

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5
ПК-3	Знает: потенциальные угрозы безопасности КИС; основные правила обеспечения безопасности рабочих станций и серверов, входящих в состав КИС; роль разработчика в построении безопасных приложений для КИС; принципиальные положения норм международного права в области авторских и смежных прав, патентного права; - содержание норм российского права в области авторских и смежных прав, патентного права; методы оценки качества	+	+	+	+	+
ПК-3	Умеет: исследовать проблемы при реализации систем безопасности КИС; настраивать почтовые сервисы (в составе КИС) для обеспечения конфиденциальности электронной переписки; обеспечивать конфиденциальность и аутентичность при взаимодействии приложений, входящих в состав программного обеспечения КИС; квалифицированно пользоваться международными документами и национального законодательства в сфере авторских и смежных прав, патентного права; оценивать угрозы информационной безопасности; определять объекты учета и оценивать затраты ИТ; рассчитывать стоимость сервиса ИТ на основе функционально- стоимостного анализа;	+	+	+	+	+
ПК-3	Имеет практический опыт: использования программных средств реализации сервисов конфиденциальности, целостности, аутентичности для КИС; использования информационно-правовых систем,	+	+			+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Суховилов, Б. М. Защита информации в корпоративных информационных системах Текст учеб. пособие к практ. работам по направлению "Приклад. информатика" Б. М. Суховилов ; Юж.-Урал. гос. ун-т, Каф. Информатика ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2013. - 39

2. Зайцев А.В. Методические указания по дисциплине "Защита информации в корпоративных информационных системах". - Челябинск, 2022

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Суховилов, Б. М. Защита информации в корпоративных информационных системах Текст учеб. пособие к практ. работам по направлению "Приклад. информатика" Б. М. Суховилов ; Юж.-Урал. гос. ун-т, Каф. Информатика ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2013. - 39

2. Зайцев А.В. Методические указания по дисциплине "Защита информации в корпоративных информационных системах". - Челябинск, 2022

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Электронно-библиотечная система издательства Лань	Ховард, М. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок. [Электронный ресурс] / М. Ховард, Д. Лебланк, Д. Виега. — Электрон. дан. — М. : ДМК Пресс, 2009. — 288 с. — Режим доступа: http://e.lanbook.com/book/1118 — Загл. с экрана.
2	Основная литература	Электронный каталог ЮУрГУ	Суховилов, Б. М. Защита информации в корпоративных информационных системах Текст учеб. пособие к практ. работам по направлению "Приклад. информатика" Б. М. Суховилов ; Юж.-Урал. гос. ун-т, Каф. Информатика ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2013. - 39, [1] с. ил. электрон. версия http://www.lib.susu.ac.ru/ftd?base=SUSU_METHOD&key=000513410
3	Основная литература	Электронно-библиотечная система издательства	Малюк, А.А. Введение в информационную безопасность. [Электронный ресурс] / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/book/5171 — Загл. с экрана.

		Лань	
4	Основная литература	Электронно-библиотечная система издательства Лань	Бирюков, А.А. Информационная безопасность: защита и нападение. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2012. — 474 с. — Режим доступа: http://e.lanbook.com/book/39990 — Загл. с экрана.

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)
3. ФГАОУ ВО "ЮУрГУ (НИУ)"-Портал "Электронный ЮУрГУ" (<https://edu.susu.ru>)(бессрочно)
4. Microsoft-Visual Studio(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Самостоятельная работа студента	258 (36)	Компьютер (ОС Windows XP, 7,8.), почтовый сервер (FreeBSD 8.3) внутри DMZ между внутренним фаерволом (FreeBSD 8.3, IPFW) и внешним фаерволом (FreeBSD 8.3, IPFW), локальная сеть кафедры с доменной инфраструктурой и выходом в Интернет, сервер сертификации (ОС Windows 2003), виртуальная машина MS Hyper-V.
Контроль самостоятельной работы	258 (36)	Компьютеры (ОС Windows XP, 7,8.), сервер тестирования AST-TEST v3.0
Экзамен	258 (36)	Компьютер (ОС Windows XP, 7,8.), почтовый сервер (FreeBSD 8.3) внутри DMZ между внутренним фаерволом (FreeBSD 8.3, IPFW) и внешним фаерволом (FreeBSD 8.3, IPFW), локальная сеть кафедры с доменной инфраструктурой и выходом в Интернет, сервер сертификации (ОС Windows 2003), виртуальная машина MS Hyper-V.
Лекции	229 (36)	Компьютер (ОС Windows XP, 7,8.) с подключенным проектором, почтовый сервер (FreeBSD 8.3) внутри DMZ между внутренним фаерволом (FreeBSD 8.3, IPFW) и внешним фаерволом (FreeBSD 8.3, IPFW), локальная сеть кафедры с доменной инфраструктурой и выходом в Интернет, сервер сертификации (ОС Windows 2003), виртуальная машина MS Hyper-V, доска для записей.
Практические занятия и семинары	258 (36)	Компьютер (ОС Windows XP, 7,8.), почтовый сервер (FreeBSD 8.3) внутри DMZ между внутренним фаерволом (FreeBSD 8.3, IPFW) и внешним фаерволом (FreeBSD 8.3, IPFW), локальная сеть кафедры с доменной инфраструктурой и выходом в Интернет, сервер сертификации (ОС Windows 2003), виртуальная машина MS Hyper-V.