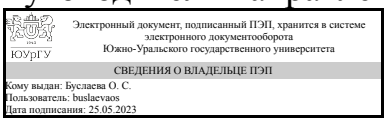
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления



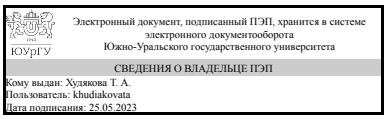
О. С. Буслаева

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

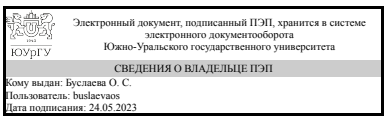
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.04.02 Информационные системы и технологии, утверждённым приказом Минобрнауки от 19.09.2017 № 917

Зав.кафедрой разработчика,
д.экон.н., доц.



Т. А. Худякова

Разработчик программы,
к.техн.н., доцент



О. С. Буслаева

Челябинск

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 обеспече-нию 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
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	69,5	69,5
Подготовка к выполнению практических заданий № 1-23	42,5	42.5
Подготовка к экзамену	27	27
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 станции.	16	8	8	0
2	Криптография симметричная и асимметричная (с открытым ключом).	20	12	8	0

	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.				
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 исполь-зовании 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 минималь¬ным необ¬ходимым 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 (зашиф-ровывание/расшифровывание). 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 Smtp (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 конфи¬денциаль¬ности 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 выполнению практических заданий № 1-23	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	1	42,5
Подготовка к экзамену	Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. ;	1	27

	Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с.		

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	Учи-тыва-ется в ПА
1	1	Проме-жуточная 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	экзамен

						компетенций. На ответы отводится 10 минут. Правильный ответ на вопрос соответствует 1 баллу. Неправильный ответ на вопрос соответствует 0 баллов.	
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. - сформление: 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	Экзамен проводится устно по билетам. Каждый билет содержит 3 вопроса, позволяющих оценить сформированность компетенций. На подготовку дается 30 минут, после чего	В соответствии с пп. 2.5, 2.6 Положения

	студент отвечает на вопросы в билете. Для уточнения уровня знаний студента преподаватель может задать от одного до трех дополнительных вопросов по темам курса. Результирующая оценка выставляется на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. При оценивании результатов учебной деятельности обучающегося по практике используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) 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 %.	

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

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

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Образовательная платформа Юрайт	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300 (дата обращения: 23.05.2023).
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	Дополнительная литература	Образовательная платформа Юрайт	Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2023. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511890 (дата обращения: 23.05.2023).
4	Основная литература	Образовательная платформа Юрайт	Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927 (дата обращения: 23.05.2023).
5	Основная литература	Образовательная платформа Юрайт	Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268 (дата обращения: 23.05.2023).
6	Дополнительная	Образовательная	Щеглов, А. Ю. Защита информации: основы теории : учебник для

	литература	платформа Юрайт	вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 (дата обращения: 23.05.2023).

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
Контроль самостоятельной работы	258 (3б)	Компьютеры (ОС Windows XP, 7,8,), сервер тестирования AST-TEST v3.0
Экзамен	258 (3б)	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 серти-фикации (ОС Windows 2003), виртуальная машина MS Hyper-V.
Лекции	229 (3б)	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 (3б)	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 серти-фикации (ОС Windows 2003), виртуальная машина MS Hyper-V.
Самостоятельная работа студента	258 (3б)	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.