Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Центр подготовки специалистов в сфере информационной безопасности и противодействия техническим средствам разведки

ОДОБРЕНО:
Руководитель ОП
_____ Е.В. Мельникова
(подпись)
«01» 09 2022 г.

Рабочая программа дисциплины

Разработка защиты сети предприятия

Уровень высшего образования:	бакалавриат
Квалификация выпускника:	бакалавр
Направление подготовки:	10.03.01 Информационная безопасность
Направленность (профиль) образовательной программы:	Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Иваново

1. Цели освоения дисциплины

Целью освоения дисциплины является формирование навыков по разработке защиты сети предприятия.

2. Место дисциплины в структуре ОП

Настоящая дисциплина Б1.В.ДВ.01.02 «Разработка защиты сети предприятия» относится к части учебного плана, формируемой участниками образовательных отношений, и является дисциплиной по выбору. Изучается на 4-м курсе в 8 семестре. Курс опирается на следующие курсы: «Организационное и правовое обеспечение информационной безопасности», «Основы управления информационной безопасностью», «Информационная безопасность организации», «Сети и системы передачи информации», «Безопасность компьютерных систем и сетей».

3. Планируемые результаты обучения по дисциплине

3.1. Компетенции, формированию которых способствует дисциплина

При освоении дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

б) профессиональные (ПК):

ПК-2 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

ПК-4 Способен принимать участие в проведении экспериментальных исследований системы защиты информации

ПК-5 Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения формируемых компетенций

В результате освоения дисциплины обучающийся должен:

Знать:

- правовые акты в области защиты информации, основные понятия и угрозы информационной безопасности, основные мероприятия по обеспечению информационной безопасности в профессиональной деятельности;
- информационно-коммуникационные технологии (ИКТ), применяемые для решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности;

Уметь:

- ориентироваться в программно-технических, правовых и организационных методах защиты сети предприятия;
- использовать методы и средства обеспечения защиты сети предприятия с целью предотвращения несанкционированного доступа, злоумышленной информации или утраты защищаемой информации;

Иметь практический опыт/Иметь навыки:

- навыками безопасного использования вычислительной техники при разработке защиты сети предприятия;
- современными общими способами обеспечения защиты сети предприятия;
- базовыми программно-аппаратными методами защиты сети предприятия.

4. Объем и содержание дисциплины

Объем дисциплины составляет 3 зачетные единицы (108 академических часов).

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа

Объем иной контактной работы и самостоятельной работы обучающегося по дисциплине указан в учебном плане образовательной программы.

№ п/п	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в ак.часах, по очной форме обучения)		Формы текущего контроля успеваемости (по очной форме обучения) Формы промежуточной аттестации
			Занятия лекцион-ного типа	Занятия семинар-ского типа	
1.	Вводный. Введение в проблематику дисциплины, представление рабочей программы, осмысление требований к организации процесса обучения, самостоятельной работы и форм аттестации	8	2		
2.	Разграничение доступа к ресурсам. Идентификация и аутентификация субъектов	8	2	6	Обсуждение результатов выполнения практической работы
3.	Хранение и распределение ключевой информации. Защита от разрушающих программных воздействий.	8	2	6	Обсуждение результатов выполнения практической работы
4.	Защита информации в компьютерных сетях	8	2	8	Обсуждение результатов выполнения практической работы
5.	Заключительное занятие	8	2		Оценка контрольной работы
Итого за семестр:			10	20	Зачет
Итого по дисциплине:			10	20	

4.2. Развернутое описание содержания дисциплины по разделам (темам)

Тема 1. Введение в дисциплину

Введение в проблематику дисциплины, представление рабочей программы, осмысление требований к организации процесса обучения, самостоятельной работы и форм аттестации.

Тема 2. Разграничение доступа к ресурсам. Идентификация и аутентификация субъектов

Политики безопасности. Дискреционные политики безопасности. Мандатные политики безопасности. Контроль доступа, базирующийся на ролях. Политика безопасности сети.

Классификация подсистем идентификации и аутентификации субъектов. Парольные системы идентификации и аутентификации пользователей.

Тема 3. Хранение и распределение ключевой информации. Защита от разрушающих программных воздействий.

Типовые схемы хранения ключевой информации. Защита баз данных аутентификации в различных ОС. Алгоритмы хеширования. Иерархия ключевой информации. Распределение ключей. Протоколы безопасной удаленной аутентификации пользователей.

Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и РПВ. Компьютерные вирусы как класс РПВ. Защита от РПВ. Изолированная программная среда.
Тема 4. Защита информации в компьютерных сетях
Основные угрозы и причины уязвимости сети Internet. Классификация типовых удаленных атак на интрасети. Ограничение доступа в сеть. Межсетевые экраны. Виртуальные частные сети (VPN). Доменная архитектура. Централизованный контроль удаленного доступа. Серверы аутентификации. Прокси-сервер.
Тема 5. Заключительное занятие
Подведение и анализ результатов освоения дисциплины

5. Образовательные технологии

Организация учебного процесса осуществляется в форме лекций, лабораторных занятий и индивидуальной самостоятельной работы студентов.
Учебный процесс по дисциплине «Разработка защиты сети предприятия» основан на использовании следующих инновационных образовательных технологий:

1. Технология проблемного обучения – основные темы курса на лекциях и лабораторных занятиях раскрываются через постановку и последующее разрешение проблемы создания алгоритма решения задачи и ее разрешение в виде функционирующей программы.
2. Технология тестового контроля качества образования – в процессе и по завершении теоретического обучения выполняется компьютерное тестирование.
3. Информационно-компьютерные технологии – применяются при выполнении лабораторных работ, самостоятельной внеаудиторной подготовке в виде самотестирования по сети Internet и использования учебных материалов в электронной форме.
4. Технология смешанного обучения.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Методика преподавания учебной дисциплины решает следующие основные задачи:
– определяет задачи обучения студентов по дисциплине;
– научно обосновывает содержание учебной программы, намечает последовательность ее изучения в комплексе с другими дисциплинами;
– определяет пути реализации принципов обучения при изучении дисциплины, формы и методы обучения;
– вырабатывает требования к методической подготовке преподавателей;
– изучает историю методики преподавания дисциплины;
– внедряет передовой опыт обучения;
– вырабатывает рекомендации по воспитанию обучаемых в процессе изучения дисциплины.
В соответствии с этими задачами осуществляется отбор научного материала, его систематизация и переработка в интересах развития и совершенствования содержания учебной дисциплины.
Методика разработана применительно к утвержденной рабочей программе для студентов с учетом требований ФГОС высшего образования по направлению подготовки 10.03.01 Информационная безопасность, и вооружает преподавателей необходимыми знаниями, способствует их внедрению в практику обучения и воспитания студентов.
Выбор методов проведения занятий обусловлен учебными целями, содержанием учебного материала, временем, отводимым на занятия.
На занятиях в тесном сочетании применяется несколько методов, один из которых выступает ведущим. Он определяет построение и вид занятий.

На лекциях излагаются лишь основные, имеющие принципиальное значение и наиболее трудные для понимания и усвоения теоретические и практические вопросы.
Теоретические знания, полученные студентами на лекциях и при самостоятельном изучении курса по литературным источникам, закрепляются при выполнении лабораторных работ.
Целями проведения лабораторных работ являются:
– приобретение практических навыков разработки защиты сети предприятия;
– контроль самостоятельной работы студентов по освоению курса;
– обучение навыкам профессиональной деятельности.
Цели лабораторных работ достигаются наилучшим образом в том случае, если им предшествует определенная подготовительная внеаудиторная работа. Поэтому преподаватель обязан довести до всех студентов график выполнения лабораторных работ с тем, чтобы они могли заниматься целенаправленной самостоятельной работой.
Работы рекомендуется выполнять в той последовательности, в которой они написаны, потому что в некоторых работах используются элементы, полученные в предыдущей работе.
На занятиях со студентами должны широко использоваться разнообразные средства обучения, способствующие более полному и правильному пониманию темы лекции или лабораторного занятия, а также выработке практических навыков по работе с ППО.
К средствам обучения студентов относятся:

- речь преподавателя;
- технические средства обучения: персональные компьютеры с установленным прикладным программным обеспечением;
- учебники, учебные пособия, лекции в электронном виде.

Полностью весь методический материал по обеспечению самостоятельной работы студентов приводится в Приложении 1 к РП.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Для контроля усвоения материала дисциплины «Разработка защиты сети предприятия» предусмотрен текущий и промежуточный контроль. Текущий контроль основан на анализе результатов выполнения лабораторных работ и собеседовании по их темам. Промежуточный контроль заключается в сдаче зачета по дисциплине.
Для проведения зачетов (экзаменов) в письменной или тестовой форме разрабатывается перечень вопросов, утверждаемый заведующим кафедрой. В перечень включаются вопросы из различных разделов курса, позволяющие проверить и оценить теоретические знания студентов и умение применять их для решения практических задач.
Зачет (экзамен) в письменной форме проводится одновременно для всех студентов академической группы. Время выполнения задания составляет не более одного академического часа.
При проведении зачета (экзамена) в письменной форме оценка выставляется на основе правил, принятых кафедрой, которые должны быть сообщены студентам до начала зачетной (экзаменационной) сессии.
Аналогичные правила могут быть заложены в программы компьютерного тестирования.
При контроле знаний в устной форме преподаватель использует метод индивидуального собеседования, в ходе которого обсуждает со студентом один или несколько вопросов из учебной программы. При необходимости могут быть предложены дополнительные вопросы, задачи и примеры. По окончании ответа на вопросы преподаватель объявляет студенту результаты сдачи зачета (экзамена).

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие: [16+] / А. М. Голиков; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с.: схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 04.12.2022). – Библиогр. в кн. – Текст: электронный.
2. Шевелев, С. С. Разработка ПО выбора параметров для мониторинга и диагностики сетевой инфраструктуры организации / С. С. Шевелев; Кубанский Государственный Технологический Университет (КубГУ). – Краснодар: б.и., 2021. – 82 с.: ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=617985 (дата обращения: 04.12.2022). – Текст: электронный.

Дополнительная литература:

1. Павлюк, В. Д. Типовые топологии вычислительных сетей / В. Д. Павлюк. – Москва: Лаборатория книги, 2011. – 105 с.: ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=142528 (дата обращения: 04.12.2022). – ISBN 978-5-504-00899-8. – Текст: электронный.
2. Бондаренко, Е. В. Компьютерные технологии: учебно-практическое пособие / Е. В. Бондаренко; Ульяновский государственный технический университет, Институт дистанционного и дополнительного образования. – Ульяновск: Ульяновский государственный технический университет (УлГТУ), 2014. – 91 с.: ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=363221 (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-9795-1238-9. – Текст: электронный.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

Система электронной поддержки образовательного процесса «Мой университет» https://uni.ivanovo.ac.ru

Профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн» www.biblioclub.ru

Электронная библиотека ИвГУ http://lib.ivanovo.ac.ru

Электронный каталог НБ ИвГУ http://lib.ivanovo.ac.ru/index.php/ek

СПС «КонсультантПлюс» http://www.consultant.ru/

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и(или) LibreOffice, интернет-браузер Microsoft Edge и(или) Yandex Browser.

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

- для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими

средствами обучения.

Лаборатория, оснащенная лабораторным оборудованием, комплектом специализированной учебной мебели и техническими средствами обучения.

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации.

Специально оборудованные кабинеты (классы, аудитории) - аудитория (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну

Специально оборудованные кабинеты (классы, аудитории) - специальная библиотека (библиотека литературы ограниченного доступа), предназначенная для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа.

ауд., лаб.	Название аудитории, лаборатории	Перечень основного используемого оборудования
457 3 корп.	Лаборатория сетей и систем передачи информации	11 рабочих мест на базе вычислительной техники с подключением к сети "Интернет" и доступом в электронную информационно-образовательную среду организации; проектор, экран на треноге;, стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов (маршрутизаторы Cisco 881, коммутаторы Cisco Catalist 2960), эмулятором (эмуляторами) активного сетевого оборудования (ПО CPT, ПО GNS), обучающее программное обеспечение ПО Putty для управления сетевым оборудованием, др.
485 3 корп.	Лаборатория технической защиты информации	11 рабочих мест на базе вычислительной техники с подключением к сети "Интернет" и доступом в электронную информационно-образовательную среду организации; проектор, экран на треноге, специализированное оборудование по защите информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок, технические средства контроля эффективности защиты информации от утечки по указанным каналам
485 3 корп.	Лаборатория программно-аппаратных средств обеспечения информационной безопасности	11 рабочих мест на базе вычислительной техники с подключением к сети "Интернет" и доступом в электронную информационно-образовательную среду организации; проектор, экран на треноге, антивирусные программные комплексы, аппаратные средства аутентификации пользователя, программно-аппаратные комплексы защиты информации, включающие в том числе криптографические средства защиты информации (АПКШ «Континент», ПАК VIPNet Coordinator, Secret Net Studio), Стенд “Шифровальные криптографические средства”, Стенд “Криптошлюзы”, Стенд “Блоки источников резервного питания”, Стенд “Системы телевизионного видеонаблюдения”, стенды для изучения проводных и беспроводных компьютерных сетей, включающие абонентские устройства, коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, системы обнаружения атак (VIPNet IDS, ПАК СОВ), межсетевые экраны, аппаратно-программные средства управления доступом к данным, шифрования (КРИПТО ПРО), др.

125 1 корп.	специально оборудованные кабинеты (классы, аудитории) информатики, технологий и методов программирования	11 рабочих мест на базе вычислительной техники с подключением к сети "Интернет" и доступом в электронную информационно-образовательную среду организации; проектор, экран на треноге, сетевым программным обеспечением, обучающим программным обеспечением

Автор(ы) рабочей программы дисциплины: Агупова Н.С., Букин Д.А., доцент Центра подготовки специалистов в сфере информационной безопасности и противодействия техническим средствам разведки, Зарубин И.А., начальник Центра подготовки специалистов в сфере информационной безопасности и противодействия техническим средствам разведки.

Программа рассмотрена и утверждена на заседании Центра подготовки специалистов в сфере информационной безопасности и противодействия техническим средствам разведки

«_____» _____ 20___г., протокол № _____

Программа обновлена
протокол заседания Центра № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ Е.В. Мельникова
(подпись)

Программа обновлена
протокол заседания Центра № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ Е.В. Мельникова
(подпись)

Программа обновлена
протокол заседания Центра № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ Е.В. Мельникова
(подпись)