Основная профессиональная образовательная программа
10.03.01 Информационная безопасность
(Безопасность компьютерных систем
(по отрасли или в сфере профессиональной деятельности))

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

Безопасность компьютерных систем и сетей

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

Основной целью изучения дисциплины является формирование знаний об объектах и задачах защиты компьютерных систем, способах и средствах нарушения информационной безопасности, о принципах и подходах к решению задач защиты информации, а также формирование умений по применению современных технологий, выбора средств и инструментов защиты информации для построения современных защищенных информационных систем и сетей в соответствии с действующим законодательством.

2. Место дисциплины в структуре ОП

Настоящая дисциплина Б1.О.39 «Безопасность компьютерных систем и сетей» относится к обязательной части учебного плана, изучается на 4-м курсе в 7,8 семестрах. Курс опирается на следующие курсы: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Программно-аппаратные средства защиты информации», «Методы и средства криптографической защиты информации», «Защита информации от утечки по техническим каналам».

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:

а) общепрофессиональные (ОПК):

ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов

ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах

ОПК-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях

ОПК-1.3 Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям.

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

В результате освоения дисциплины обучающийся должен:

Знать:

- принципы функционирования защищенных компьютерных сетей;
- требования к обеспечению защищенности компьютерных сетей;
- требования эффективного функционирования средств защиты информации в компьютерных системах и сетях;
- современные угрозы сетевой безопасности в корпоративных вычислительных сетях;

Уметь:

- проводить анализ и оценку защищенности компьютерных сетей;
- администрировать средства защиты информации в компьютерных системах и сетях;
- проводить мониторинг угроз безопасности информации в компьютерных системах и сетях.

Иметь практический опыт/Иметь навыки:

- выбора средств обеспечения информационной безопасности информационной системы современного предприятия;
- организации защиты информации в локальной сети.

4. Объем и содержание дисциплины

Объем дисциплины составляет 5 зачетных единиц (180 академических часов), в т.ч. практическая подготовка (ПП) – 12 академических часов в очной форме.

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 лекционного типа	Занятия семинарского типа	
1.	Вводный. Введение в проблематику дисциплины, представление рабочей программы, осмысление требований к организации процесса обучения, самостоятельной работы и форм аттестации	7	2		Входная диагностика: тест с последующим обсуждением результатов. Список вопросов, интересующих студента по содержанию дисциплины (сдается в письменном виде)
2.	Современные угрозы сетевой безопасности.	7	2	1	Обсуждение результатов выполнения лабораторной работы
3.	Обеспечение безопасности сети.	7	2	1	Обсуждение результатов выполнения лабораторной работы
4.	Сетевые угрозы. Вредоносное ПО. Распространенные сетевые атаки.	7	2	1	Обсуждение результатов выполнения лабораторной работы

5.	Защита сети, области сетевой безопасности. Устранение типичных сетевых атак.	7	2	1	Обсуждение результатов выполнения лабораторной работы
6.	Обеспечение безопасности сетевых устройств. Защита доступа к устройствам.	7	2	1	Обсуждение результатов выполнения лабораторной работы
7.	Назначение административных ролей. Мониторинг устройств и управление ими.	7	2	1	Обсуждение результатов выполнения лабораторной работы
8.	Использование автоматических функций обеспечения безопасности. Защита плоскости управления.	7	2	1	Обсуждение результатов выполнения лабораторной работы
9.	Аутентификация, авторизация и учет (AAA). Назначение AAA.	7	2	1	Обсуждение результатов выполнения лабораторной работы
10.	Локальная аутентификация AAA.	7	2	1	Обсуждение результатов выполнения лабораторной работы
11.	Серверное решение AAA. Серверная аутентификация AAA. Серверная авторизация и учет AAA.	7	2	1	Обсуждение результатов выполнения лабораторной работы
12.	Внедрение технологий межсетевого экранирования. Эволюция систем межсетевого экранирования.	7	2	1	Обсуждение результатов выполнения лабораторной работы
13.	Списки контроля доступа.	7	2	1	Обсуждение результатов выполнения лабораторной работы
14.	Типы межсетевых экранов. Зональные межсетевые экраны.	7	2	1	Обсуждение результатов выполнения лабораторной работы
15.	Внедрение системы предотвращения вторжений (IPS). Технология IPS. Варианты сетевой реализации IPS.	7	2	1	Обсуждение результатов выполнения лабораторной работы
16.	Сигнатуры IPS. Действия сигнатур. Внедрение IPS. Проверка и мониторинг IPS.	7	2	1	Обсуждение результатов выполнения лабораторной работы
17.	Обеспечение безопасности локальной сети. Безопасность оконечных устройств.	7		1	Обсуждение результатов выполнения лабораторной работы
Итого за 7 семестр:			32	16	Зачет
1.	Нейтрализация атак на таблицу CAM. Нейтрализация атак на сеть VLAN.	8	2	3	Обсуждение результатов выполнения практической работы
2.	Нейтрализация атак DHCP. Нейтрализация атак ARP.	8	2	3	Обсуждение результатов выполнения практической работы

3.	Нейтрализация атак спуфинга адресов. Нейтрализация атак STP.	8	2	3	Обсуждение результатов выполнения практической работы
4.	Внедрение виртуальных частных сетей. Сети VPN, типы.	8	2	3	Обсуждение результатов выполнения практической работы
5.	Компоненты сети IPsec и их функционирование.	8	2	3	Обсуждение результатов выполнения практической работы
6.	Реализация сетей IPsec между двумя пунктами.	8	2	3	Обсуждение результатов выполнения практической работы
7.	Внедрение многофункциональных устройств защиты.	8	2	3	Обсуждение результатов выполнения практической работы
8.	Базовая конфигурация. Конфигурация межсетевого экрана.	8	2	3	Обсуждение результатов выполнения практической работы
9.	Настройка AAA. Настройка сервисных политик.	8	2	3	Обсуждение результатов выполнения практической работы
10.	Настройка ACL.	8	2	3	Обсуждение результатов выполнения практической работы
Итого за 8 семестр:			20	30	Экзамен
Итого по дисциплине:			52	46	

4.2. Развернутое описание содержания дисциплины по разделам (темам)

Современные угрозы сетевой безопасности. Обеспечение безопасности сети. Сетевые угрозы. Вредоносное ПО. Распространенные сетевые атаки. Защита сети, области сетевой безопасности. Устранение типичных сетевых атак.

Обеспечение безопасности сетевых устройств. Защита доступа к устройствам. Назначение административных ролей. Мониторинг устройств и управление ими. Использование автоматических функций обеспечения безопасности. Защита плоскости управления.

Аутентификация, авторизация и учет (AAA). Назначение AAA. Локальная аутентификация AAA. Серверное решение AAA. Серверная аутентификация AAA. Серверная авторизация и учет AAA.

Внедрение технологий межсетевого экранирования. Эволюция систем межсетевого экранирования. Списки контроля доступа. Типы межсетевых экранов. Зональные межсетевые экраны.

Внедрение системы предотвращения вторжений (IPS). Технология IPS. Варианты сетевой реализации IPS. Сигнатуры IPS. Действия сигнатур. Внедрение IPS. Проверка и мониторинг IPS.

Обеспечение безопасности локальной сети. Безопасность оконечных устройств. Нейтрализация атак на таблицу CAM. Нейтрализация атак на сеть VLAN. Нейтрализация атак DHCP. Нейтрализация атак ARP. Нейтрализация атак спуфинга адресов. Нейтрализация атак STP.

Внедрение виртуальных частных сетей. Сети VPN, типы. Компоненты сети IPsec и их функционирование. Реализация сетей IPsec между двумя пунктами.

Внедрение многофункциональных устройств защиты. Базовая конфигурация. Конфигурация межсетевого экрана. Настройка AAA. Настройка сервисных политик. Настройка ACL.

5. Образовательные технологии

Организация учебного процесса осуществляется в форме лекций, лабораторных занятий и индивидуальной самостоятельной работы студентов.

Учебный процесс по дисциплине «Безопасность компьютерных систем и сетей» 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 выбора средств обеспечения информационной безопасности информационной системы современного предприятия и организации защиты информации в локальной сети;

– 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 «Безопасность компьютерных систем и сетей» 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 и экзамена 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. Демидов, Л. Н. Основы эксплуатации компьютерных сетей: учебник для бакалавров / Л. Н. Демидов. – Москва : Прометей, 2019. – 799 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576033 (дата обращения: 04.12.2022). – Библиогр.: с. 750 - 752. – ISBN 978-5-907100-01-5. – Текст : электронный.
2. Сысоев, Э. В. Администрирование компьютерных сетей : учебное пособие / Э. В. Сысоев, А. В. Терехов, Е. В. Бурцева. – Тамбов : Тамбовский государственный технический

университет (ТГТУ), 2017. – 80 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499414 (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-8265-1802-1. – Текст : электронный.

Дополнительная литература:

1. Прохорова, О. В. Информационная безопасность и защита информации : учебник : [16+] / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.
2. Основы администрирования информационных систем : учебное пособие : [16+] / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 202 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-4499-1674-7. – DOI 10.23681/598955. – Текст : электронный.
3. Сети и системы телекоммуникаций: учебное электронное издание : учебное пособие : [16+] / В. А. Погонин, А. А. Третьяков, И. А. Елизаров, В. Н. Назаров. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 197 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=570531 (дата обращения: 04.12.2022). – Библиогр.: с. 190-191. – ISBN 978-5-8265-1931-8. – 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)