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

Криптографические протоколы

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 ознакомление студентов с основными криптографическими протоколами; развитие навыка построения криптографического протокола из элементарных протоколов, и развития логического мышления в рамках этой задачи; овладение навыком разложения любого криптографического протокола на промежуточные с целью создания программного обеспечения, обслуживающего исполнение протокола.

2. Место дисциплины в структуре ОП

Настоящая дисциплина Б1.О.38 «Криптографические протоколы» относится к обязательной части учебного плана, изучается на 3-м курсе в 5 семестре. Курс опирается на следующие курсы: «Алгебраические основы криптографии», «Основы информационной безопасности» и «Операционные системы».

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

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.

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

В результате освоения дисциплины обучающийся должен:

Знать:

- методы построения криптографических протоколов и алгоритмов;
- основные типы атак на криптографические протоколы;

Уметь:

- выбирать криптографические протоколы в соответствии с требованиями безопасности и производительности;
- формулировать требования к криптографическому протоколу, обеспечивающему безопасность компьютерной системы;

Иметь практический опыт/Иметь навыки:

- применять криптографические протоколы с учетом требований нормативных и правовых актов по защите информации;
- использовать криптографические протоколы

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 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	5	2		Входная диагностика: тест с последующим обсуждением результатов. Список вопросов, интересующих студента по содержанию дисциплины (сдается в письменном виде)
2.	Криптографические протоколы и основные требования к ним.	5	2	2	Обсуждение результатов выполнения лабораторной работы
3.	Основные атаки на криптографические протоколы.	5	2	2	Обсуждение результатов выполнения лабораторной работы
4.	Понятие протокола в криптографии. Классификация криптографических протоколов.	5	2	2	Обсуждение результатов выполнения лабораторной работы
5.	Понятие атаки на криптографический протокол. Основные атаки на криптографические протоколы.	5	2	2	Обсуждение результатов выполнения лабораторной работы
6.	Доказательства с нулевым разглашением. Разглашение знаний.	5	2	2	Обсуждение результатов выполнения лабораторной работы
7.	Полное, частичное минимальное и нулевое разглашение.	5	2	2	Обсуждение результатов выполнения лабораторной работы
8.	Подбрасывание монеты по телефону. Диалоговые и бездиалоговые протоколы доказательства с нулевым разглашением.	5	2	2	Обсуждение результатов выполнения лабораторной работы
9.	Доказательство знания разложения составного числа на множители.	5	2	2	Обсуждение результатов выполнения лабораторной работы
10.	Доказательство знания дискретного логарифма.	5	2	2	Обсуждение результатов выполнения лабораторной работы
11.	Схемы электронного голосования на основе доказательства с нулевым разглашением.	5	2	2	Обсуждение результатов выполнения лабораторной работы

12.	Схемы электронной подписи.	5	2	2	Обсуждение результатов выполнения лабораторной работы
13.	Разовые подписи. Неоспоримая подпись.	5	2	2	Обсуждение результатов выполнения лабораторной работы
14.	Личностные схемы. Online-offline-подпись.	5	2	2	Обсуждение результатов выполнения лабораторной работы
15.	Схемы коллективной аутентификации.	5	2	2	Обсуждение результатов выполнения лабораторной работы
16.	Способы организации коллективной аутентификации.	5	2	2	Обсуждение результатов выполнения лабораторной работы
17.	Схемы групповой, кольцевой, пороговой, упорядоченной подписи.	5	2	2	Обсуждение результатов выполнения лабораторной работы
Итого за семестр:					Зачет
Итого по дисциплине:			36	32	

4.2. Развернутое описание содержания дисциплины по разделам (темам)

Криптографические протоколы и основные требования к ним. Основные атаки на криптографические протоколы. Понятие протокола в криптографии. Классификация криптографических протоколов. Понятие атаки на криптографический протокол. Основные атаки на криптографические протоколы.

Доказательства с нулевым разглашением. Разглашение знаний. Полное, частичное минимальное и нулевое разглашение. Подбрасывание монеты по телефону. Диалоговые и бездиалоговые протоколы доказательства с нулевым разглашением. Доказательство знания разложения составного числа на множители. Доказательство знания дискретного логарифма. Схемы электронного голосования на основе доказательства с нулевым разглашением.

Схемы электронной подписи. Разовые подписи. Неоспоримая подпись. Личностные схемы. Online-offline-подпись.

Схемы коллективной аутентификации. Способы организации коллективной аутентификации.

Схемы групповой, кольцевой, пороговой, упорядоченной подписи.

5. Образовательные технологии

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

Учебный процесс по дисциплине «Криптографические протоколы» 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 работы с криптографическими протоколами;

– 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 «Криптографические протоколы» 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. Майстренко, Н. В. Основы теории информации и криптографии: учебное электронное издание : учебное пособие / Н. В. Майстренко, А. В. Майстренко. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 81 с. : табл., граф., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=570354 (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-8265-1950-9. – Текст : электронный.
2. Фороузан, Б. А. Математика криптографии и теория шифрования : учебное пособие : [16+] / Б. А. Фороузан. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 511 с. : ил., схем. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428998 (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-9963-0242-0. – Текст : электронный.
3. Кнауб, Л. В. Теоретико-численные методы в криптографии : учебное пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов ; Сибирский федеральный университет. – Красноярск : Сибирский федеральный университет (СФУ), 2011. – 160 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=229582 (дата обращения: 04.12.2022). – ISBN 978-5-7638-2113-7. – Текст : электронный.

Дополнительная литература:

1. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование : учебное пособие : [16+] / А. В. Аграновский, Р. А. Хади. – Москва : СОЛОН-ПРЕСС, 2009.

– 256 с. – (Аспекты защиты). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=117663 (дата обращения: 04.12.2022). – ISBN 5-98003-002-6. – Текст : электронный.

2. Лидовский, В. В. Основы теории информации и криптографии: курс : учебное пособие : [16+] / В. В. Лидовский ; Национальный Открытый Университет "ИНТУИТ". – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2007. – 125 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=234148 (дата обращения: 04.12.2022). – 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)