Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный индустриальный университет»

Кафедра менеджмента качества и инноваций

УТВЕРЖДАЮ
Директор института передовых инженерных технологий
_____ И.Ю. Кольчурина
подпись
«____» _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Кибербезопасность и защита данных

09.03.02 «Информационные системы и технологии»
(направленность (профиль): «Системный анализ и управление цифровыми проектами»)

Квалификация выпускника
Бакалавр

Форма обучения
Очная форма

Срок обучения: 4 года

Год начала подготовки 2026

Новокузнецк
2026

СибГИУ
Подлинник электронного документа хранится в системе электронного согласования документов СибГИУ
ДОКУМЕНТ ПОДПИСАН ЭП
Сертификат: c7fcee22ea712e8a9d62ca0595e78e8dabbfaa85
Владелец: Директор ИПИТ Кольчурина Ирина Юрьевна
Действителен: с 4 июня 2025 г. по 26 августа 2026 г.
Дата и время: 03-06-2026 14:16:17 ПРОВЕРИТЬ ПОДПИСЬ

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

– формирование системного представления о современных угрозах информационной безопасности, принципах и методах защиты данных в информационных системах;
– приобретение знаний, умений и навыков по обеспечению кибербезопасности, управлению доступом, криптографической защите и противодействию атакам.

Задачами учебной дисциплины являются:

– формирование представлений о роли и месте кибербезопасности в автоматизированных системах, о назначении и основных характеристиках средств защиты информации;
– знакомство с основными принципами идентификации, аутентификации, авторизации, разграничения доступа;
– изучение криптографических методов защиты данных (симметричное и асимметричное шифрование, электронная подпись, хеширование);
– освоение методов защиты сетевой инфраструктуры (межсетевые экраны, IDS/IPS, VPN);
– формирование практических навыков анализа уязвимостей, реагирования на инциденты и обеспечения безопасности приложений.

2 Место учебной дисциплины в структуре ООП по направлению подготовки (специальности)

Учебная дисциплина относится к учебным дисциплинам обязательной части **Блока 1 «Дисциплины (модули)»** ООП по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

– Введение в информационные системы;
– Технологии программирования;
– Базы данных;
– Администрирование информационных систем.

Учебная дисциплина дополняет знания и умения, получаемые по одновременно изучаемым и последующим учебным дисциплинам:

– Архитектура промышленных информационных систем;
– Управление IT-проектами;
– Моделирование бизнес-процессов;
– Производственная практика;
– Подготовка к сдаче и сдача государственного экзамена.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

– Общепрофессиональные компетенции

Наименование категории (группы) ОПК	Код и наименование ОПК	Код и наименование индикатора достижения ОПК	Планируемые результаты обучения
	ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1 Осуществляет поиск информационных ресурсов для решения типовых профессиональных задач с учетом требований информационной безопасности	– знать: основные угрозы информационной безопасности при поиске информации в сетях и локальных хранилищах, типовые уязвимости информационных ресурсов. – уметь: осуществлять поиск профессиональных информационных ресурсов (научных статей, технической документации, нормативных актов) с учётом требований информационной безопасности, применять инструменты для проверки подлинности источников.
		ОПК-3.2 Выбирает актуальные и достоверные источники информации с учетом основных требований информационной безопасности	– знать: методы проверки целостности и подлинности источников данных (контрольные суммы, ЭЦП, репутационные сервисы). – уметь: оценивать уровень доверия к источнику информации (сайт, документ, база данных) на основе анализа сертификатов,

			домена, наличия лицензии, применять инструменты верификации.
		ОПК-3.3 Решает стандартные задачи профессиональной деятельности, применяя достоверную информацию из различных источников с учетом требований информационной безопасности	– знать: методы обеспечения информационной безопасности при решении стандартных профессиональных задач (работа с базами данных, сетевое администрирование, программирование, обработка персональных данных), принципы безопасного хранения, обработки и передачи данных (шифрование, резервное копирование, контроль доступа). – уметь: решать профессиональные задачи (например, администрирование БД, настройка серверов, разработка приложений) с применением средств защиты информации (межсетевые экраны, шифрование, DLP-системы), выбирать адекватные меры защиты в зависимости от класса обрабатываемой информации и угроз.

4 Объем и содержание учебной дисциплины

Учебные занятия по учебной дисциплине проводятся в форме контактной работы и в форме самостоятельной работы обучающихся.

Контактная работа включает в себя занятия лекционного типа (лекции), занятия семинарского типа (семинары, практические занятия, практикумы), промежуточную аттестацию обучающихся и иные формы

взаимодействия обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации ООП на иных условиях, в том числе при проведении промежуточной аттестации обучающихся. Контактная работа может проводиться с применением электронного обучения, дистанционных образовательных технологий.

Объем учебной дисциплины

Семестр / курс		***ИТОГО***	***5 семестр***
Форма промежуточной аттестации			*зачет с оценкой*
Трудоёмкость	*академ. час.*	***108***	*108*
	зачетных единиц	***3***	*3*
Лекции, *академ. час.*		***16***	*16*
в форме практической подготовки		***0***	*0*
Лабораторные работы, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Практические занятия, *академ. час.*		***32***	*32*
в форме практической подготовки		***0***	*0*
Курсовая работа / проект, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Консультации, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Самостоятельная работа, *академ. час.*		***51***	*51*
в форме практической подготовки		***0***	*0*
Контроль, *академ. час.*		***9***	*9*
в форме практической подготовки		***0***	*0*

Содержание учебной дисциплины

Раздел 1 Введение в кибербезопасность;

Тема 1.1 Основные понятия информационной безопасности (конфиденциальность, целостность, доступность). Классификация угроз. Модели нарушителя.;

Тема 1.2 Нормативно-правовая база в области защиты данных (ФЗ-152 «О персональных данных», ФЗ-187 «О безопасности КИИ», стандарты серии ГОСТ/ISO).;

Раздел 2 Криптографические методы защиты информации;

Тема 2.1 Симметричное шифрование (алгоритмы DES, AES). Режимы шифрования. Управление ключами.;

Тема 2.2 Асимметричное шифрование (RSA, ECC). Электронная подпись. Хеш-функции (MD5, SHA). Применение в SSL/TLS.;

Раздел 3 Управление доступом и идентификация;

Тема 3.1 Мандатное, дискреционное и ролевое управление доступом. Модели Белла – Лападулы, Кларка – Уилсона.;

Тема 3.2 Многофакторная аутентификация. Биометрическая защита. Управление паролями. Протоколы аутентификации (Kerberos, RADIUS).;

Тема 3.3 Политики информационной безопасности. Управление инцидентами. План действий при утечке данных;

Раздел 4 Сетевая безопасность;

Тема 4.1 Межсетевые экраны (фильтрующие, прокси, NGFW). Правила фильтрации. Технологии NAT.;

Тема 4.2 Системы обнаружения и предотвращения вторжений (IDS/IPS). Анализ сетевого трафика. VPN (IPsec, OpenVPN).;

Раздел 5 Безопасность приложений и веб-безопасность;

Тема 5.1 Уязвимости веб-приложений (OWASP Top 10): SQL-инъекции, XSS, CSRF. Методы защиты.;

Тема 5.2 Безопасное программирование. Статический и динамический анализ кода. Защита от переполнения буфера.;

Тема 5.3 Резервное копирование и восстановление. Шифрование данных на диске и в облаке. DLP-системы.

5 Перечень тем лекций

№ раздела / темы дисциплины	Темы лекций	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Раздел 1.	Основы информационной безопасности. Угрозы и уязвимости. Нормативно-правовое регулирование в области защиты данных.	4	
Раздел 2.	Симметричное шифрование. Алгоритмы DES, AES. Асимметричное шифрование. Электронная подпись. Хеширование.	4	
Раздел 3.	Управление доступом. Дискреционное, мандатное, ролевое. Аутентификация. Многофакторная защита. Протоколы.	4	
Раздел 4.	Межсетевые экраны. Принципы работы и конфигурация.	2	
Раздел 5.	Системы обнаружения вторжений (IDS/IPS). VPN.	2	
Итого:		**16**	**0**

6 Перечень тем практических занятий (семинаров)

№ раздела / темы	Темы практических	Трудоемкость, *академ.час*

дисциплины	занятий (семинаров)	всего	в форме практической подготовки
Раздел 1.	Анализ угроз информационной безопасности и построение модели нарушителя	4	
Раздел 2.	Практическая реализация симметричного шифрования (AES) на языке Python	4	
Раздел 3.	Настройка дискреционного и ролевого доступа в ОС. Политики резервного копирования	4	
Раздел 4.	Анализ сетевого трафика с помощью Wireshark. Обнаружение атак.	6	
Раздел 5.	Тестирование веб-приложений на SQL-инъекции и XSS	8	
Раздел 2.	Реализация алгоритма RSA. Генерация и проверка ЭП.	6	
Итого:		**32**	**0**

7 Перечень тем лабораторных работ

№ раздела / темы дисциплины	Темы лабораторных работ	Трудоемкость, *академ.час*	
		всего	в форме практической подготовки
	Отсутствуют		
Итого:		**0**	**0**

8 Перечень тем курсовых работ (проектов)

№ раздела / темы дисциплины	Темы курсовых работ (проектов)	Трудоемкость, *академ.час*	
		всего	в форме практической подготовки
	Отсутствуют		
Итого:		**0**	**0**

9 Виды самостоятельной работы

№ раздела / темы дисциплины	Виды самостоятельной работы	Трудоемкость, *академ.час*	
		всего	в форме практической подготовки

Раздел 1.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	8	
Раздел 2.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	10	
Раздел 3.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	10	
Раздел 4.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	13	
Раздел 5.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	10	
Контроль	*Подготовка к зачёту*	9	
Итого:		**60**	**0**

10 Матрица компетентностных задач по учебной дисциплине

Контролируемые разделы (темы) дисциплины	Контролируемые компетенции	Оценочные средства
Раздел 1.	ОПК-3	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Тестовые задания
Раздел 2.	ОПК-3	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Тестовые задания
Раздел 3.	ОПК-3	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии;

		3. Тестовые задания
Раздел 4.	ОПК-3	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Тестовые задания
Раздел 5.	ОПК-3	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Тестовые задания
Зачет с оценкой.	ОПК-3	1. Зачет с оценкой на основе результатов компьютерного тестирования; 2. Зачет с оценкой на основе результатов текущего контроля

11 Входной контроль

11.1 Цель входного контроля − определить начальный уровень подготовленности обучающихся и выстроить индивидуальную траекторию обучения. В условиях личностно-ориентированной образовательной среды результаты входного оценивания обучающегося используются как начальные значения в индивидуальном профиле академической успешности обучающегося.

11.2 Описание оценочных средств

Форма проведения входного контроля – тестирование.

Длительность тестирования – 20 минут.

Тестирование проводится в течение первых двух недель изучения учебной дисциплины в СУО СибГИУ.

Для проведения тестирования используются тестовые задания для входного контроля (для ответа на 1 вопрос, как правило, выделяется 1 минута).

Шкала оценивания результатов тестирования

За каждый правильный ответ выставляется 1 балл. Оценка выставляется в зависимости от процента правильных ответов:

Оценка формируется в соответствии с критериями таблицы:

Процент результативности (правильных ответов)	Оценка
86 до 100	«отлично»
от 67до 85	«хорошо»
от 50 до 66	«удовлетворительно»
менее 50	«неудовлетворительно»

Основываясь на результатах тестирования, формируется индивидуальная траектория обучающегося (группы обучающихся), исходя из следующих соображений:

– 86 – 100 % – обучающийся готов к изучению учебной дисциплины без дополнительного повторения изученного ранее материала;

– 50 – 67 % – обучающийся в целом готов к изучению учебной дисциплины, требуется повторение отдельных вопросов(тем) изученного ранее материала, необходимого для успешного освоения учебной дисциплины;

– 49% и менее – обучающийся имеет слабую подготовку к изучению учебной дисциплины, необходимы корректирующие занятия и консультации.

Тестовые задания для входного контроля знаний обучающихся приведены в приложении.

12 Текущий контроль

12.1 Текущий контроль знаний используется для оперативного и регулярного управления учебной деятельностью (в том числе самостоятельной) обучающихся. Данный вид контроля стимулирует у обучающихся стремление к систематической самостоятельной работе по изучению учебной дисциплины и позволяет оценить степень освоения изученного материала.

Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы по индивидуальной инициативе педагогического работника, в том числе посредством использования СУО СибГИУ.

Формы проведения текущего контроля – вопросы для устного обсуждения (опроса); наблюдение за работой на практическом занятии; тестовые задания.

12.2 Описание оценочных средств

Шкалы оценивания (методики оценки)

12.2.1 Рекомендации по оцениванию устных ответов обучающихся

С целью контроля и подготовки обучающихся к изучению новой темы в начале занятия лекционного типа (лекции) педагогическим работником проводится индивидуальный или фронтальный устный опрос по выполненным заданиям предыдущего раздела (темы).

Критерии оценки:

– правильность ответа по содержанию задания (учитывается количество и характер ошибок при ответе);

– полнота и глубина ответа (учитывается количество усвоенных фактов, понятий и т.п.);

– сознательность ответа (учитывается понимание излагаемого материала);

– логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией);

– рациональность использованных приемов и способов решения поставленной учебной задачи (учитывается умение использовать наиболее прогрессивные и эффективные способы достижения цели);

– своевременность и эффективность использования наглядных пособий и технических средств при ответе (учитывается умение грамотно и с пользой применять наглядность и демонстрационный опыт при устном ответе);

– использование дополнительного материала (обязательное условие);

– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения задания, устного ответа во времени).

Оценка «отлично» ставится, если обучающийся:

– полно и аргументировано отвечает по содержанию задания;

– обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры, в том числе самостоятельно составленные;

– излагает материал последовательно и правильно.

Оценка «хорошо» ставится, если обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1 – 2 ошибки, которые сам же исправляет.

Оценка «удовлетворительно» ставится, если обучающийся обнаруживает знание и понимание основных положений данного задания, но:

– излагает материал неполно и допускает неточности в определении понятий или формулировке правил;

– не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;

– излагает материал непоследовательно и допускает ошибки.

Оценка «неудовлетворительно» ставится, если обучающийся обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Оценка «неудовлетворительно» отмечает такие недостатки в подготовке обучающегося, которые являются серьезным препятствием к успешному освоению последующего материала.

12.2.2 Рекомендации по оцениванию результатов тестирования обучающихся

Тестирование проводится по изученным разделам (темам) учебной дисциплины для выявления уровня знаний и умений обучающегося, мотивирования обучающегося к активизации самостоятельной работы по усвоению учебного материала, выявления и устранения пробелов в знаниях, повышения дисциплины и организации учебной деятельности обучающегося.

Тестирование проводится в СУО СибГИУ в рамках часов, отведенных на самостоятельную работу обучающихся. Для тестирования используется 20 вопросов из базы типовых тестовых заданий по изученным разделам (темам) учебной дисциплины. Обучающийся выбирает один ответ из предложенных вариантов ответа. В случае выбора неправильного ответа обучающийся получает за данный вопрос 0 баллов; в случае правильного ответа – 1 балл.

Оценка формируется в соответствии с критериями таблицы:

Максимальный балл	Проходной балл	Оценка
20	не менее 18	отлично
17	не менее 14	хорошо
13	не менее 10	удовлетворительно
9	–	неудовлетворительно

12.2.3 Рекомендации по оцениванию в процессе наблюдения за работой на практическом занятии

Наблюдение за работой на практическом занятии – важнейший компонент контроля деятельности обучающихся и качества их обучения.

Критерии оценки в процессе наблюдения за работой на практическом занятии:

– самостоятельность выполнения задания и работы с методическими указаниями (учитывается работа в течение занятия, быстрота и способность нахождения в методических указаниях нужной информации);

– правильность выполнения работы (учитывается последовательность выполняемых действий, умение работать с инструментами и/или средствами вычислительной техники);

– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения работы с учетом индивидуальных особенностей обучающихся);

– активность обучающегося при выполнении практической работы (учитывается индивидуальная работа и работа в группе).

Критерии оценки по результатам наблюдения за работой на практическом занятии

Наименование параметра оценки	Максимальное количество баллов
Самостоятельно выполняет задания; умеет работать с методическими указаниями.	2,5
Указанные в методических указаниях действия выполняет в правильной последовательности; умеет работать с инструментами и/или средствами вычислительной техники.	1,25
Рационально использует время, отведенное на задание; проявляет активность при выполнении практической работы.	1,25
Итого	**5**

Максимальное количество – 5 баллов соответствует оценке «отлично», 4 балла – «хорошо», 3 балла – «удовлетворительно», 2 балла – «неудовлетворительно».

Задания и вопросы для текущего контроля знаний обучающихся по разделам (темам) учебной дисциплины приведены в приложении.

13 Промежуточная аттестация

13.1 Оценочные материалы для промежуточной аттестации обучающихся по учебной дисциплине предназначены для оценки степени достижения запланированных результатов обучения по завершению изучения учебной дисциплины в установленной учебным планом форме и позволяют определить качество усвоения изученного материала.

Итоговой формой контроля сформированности компетенций у обучающихся по учебной дисциплине является: зачет с оценкой.

Оценочные материалы для промежуточной аттестации обучающихся включают: зачет с оценкой на основе результатов компьютерного тестирования; зачет с оценкой на основе результатов текущего контроля.

13.2 Оценивание обучающегося на зачете с оценкой

Оценка	Требования к знаниям
отлично	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал различной литературы, правильно обосновывает принятое нестандартное решение, обладает приемами выполнения практических задач по формированию компетенций.
хорошо	Оценка «хорошо» выставляется обучающемуся, если он

Оценка	Требования к знаниям
	твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, обладает необходимыми умениями и приемами их выполнения.
удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает сложности при выполнении практических работ и затрудняется связать теорию вопроса с практикой.
неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, неуверенно отвечает, допускает серьезные ошибки, не имеет представлений по методике выполнения практической работы. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по данной учебной дисциплине.

Задания и вопросы для промежуточной аттестации обучающихся приведены в приложении.

14 Учебно-методическое и информационное обеспечение учебной дисциплины

а) литература:

1 Козырь, Н. С. Информационные технологии в кибербезопасности : учебник для вузов / Н. С. Козырь, А. М. Левченко. — Москва : Издательство Юрайт, 2026. — 217 с. — (Высшее образование). — ISBN 978-5-534-22095-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/600794 (дата обращения: 09.02.2026);

2 Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/589902 (дата обращения: 09.02.2026);

3 Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/588741 (дата обращения: 09.02.2026);

4 Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов,

С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/583236 (дата обращения: 09.02.2026);

5 Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/583236 (дата обращения: 09.02.2026).

б) ресурсы информационно-телекоммуникационной сети «Интернет»:

1 Электронный каталог : сайт / Научно-техническая библиотека СибГИУ. – Новокузнецк, [199 –]. – URL: http://libr.sibsiu.ru. – URL: https://libr.sibsiu.ru;

2 Электронная библиотека // Научно-техническая библиотека СибГИУ : сайт. – Новокузнецк, [200 –]. – URL: http://library.sibsiu.ru/LibrELibraryFullText.asp. – Режим доступа: для авторизир. пользователей. – URL: https://library.sibsiu.ru/LibrELibraryFullText.asp;

3 Консультант студента : электронно-библиотечная система / ООО «КОНСУЛЬТАНТ СТУДЕНТА». – Москва, [200 –]. – URL: http://www.studentlibrary.ru. – Режим доступа: для авторизир. пользователей;

4 ЛАНЬ : электронно-библиотечная система : [коллекция «Единая профессиональная база знаний для технических вузов - Издательство Лань" ЭБС»] / ООО «Издательство ЛАНЬ». – Санкт-Петербург, [200 –]. – URL: http://e.lanbook.com. – Режим доступа: для авторизир. пользователей;

5 Образовательная платформа ЮРАЙТ / ООО «Электронное издательство ЮРАЙТ». – Москва, [200 –]. – URL: https://urait.ru. – Режим доступа: для авторизир. пользователей;

6 Университетская библиотека онлайн : электронно-библиотечная система / ООО «Директ-Медиа». – Москва, [200 –]. – URL: https://biblioclub.ru. – Режим доступа: для авторизир. пользователей. – URL: http://www.biblioclub.ru;

7 НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU : база данных / ООО «НЭБ». – Москва, [200 –]. – URL: http://elibrary.ru. – Режим доступа: по подписке;

8 Электронные периодические издания ИВИС : универсальная база данных / ООО «ИВИС». – Москва, [200 –]. – URL: http://eivis.ru. – Режим доступа: по подписке.

в) лицензионное и свободно распространяемое программное обеспечение:

– 7-Zip;
– Adobe Acrobat Reader;
– Astra Linux Special Edition;
– Kaspersky Endpoint Security;
– Microsoft Office;
– Microsoft Windows;
– OnlyOffice;
– Р7-Офис.

г) базы данных и информационно-справочные системы:

1 ГАРАНТ : справочно-правовая система / ООО «Правовой центр «Гарант». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.;

2 КонсультантПлюс : справочно-правовая система / ООО «Информационный центр АНВИК». – Новокузнецк, [199 –]. – Режим доступа: компьютерная сеть библиотеки Сиб. гос. индустр. ун-та.;

3 Техэксперт : информационно-справочная система / ООО «Группа компаний «Кодекс». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.

15 Материально-техническое обеспечение учебной дисциплины

Материально-техническое обеспечение учебной дисциплины включает учебные аудитории, оснащенные оборудованием, компьютерной техникой, и техническими средствами обучения, в том числе:

- учебную аудиторию для проведения занятий лекционного типа, оборудованную учебной доской, экраном и мультимедийным проектором;
- учебную аудиторию для проведения занятий семинарского типа (практических занятий), оснащенную ПК с доступом в Интернет, ОС Linux и Windows, установленное ПО для сетевого анализа и криптографии);
- учебную аудиторию (помещения) для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду, научно-техническую библиотеку СибГИУ.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии».

Составитель(и):

доцент Корнева Анна Валерьевна (кафедра прикладной математики и информатики).

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры.

Согласован:

зав. кафедрой информатики и общетехнических дисциплин КГПИ КемГУ
к.пед.н., доцент  И.В. Сликишина

Приложение

Тестовые задания для входного контроля знаний обучающихся

Выберите один правильный ответ.

1. Что из перечисленного НЕ относится к трём основным свойствам информационной безопасности (триада CIA)?

A) Конфиденциальность
B) Целостность
C) Доступность
D) Неотказуемость

2. Какой алгоритм шифрования относится к симметричному?

A) RSA
B) AES
C) ECDSA
D) Diffie-Hellman

3. Для чего в первую очередь предназначена технология VPN?

A) Для увеличения скорости передачи данных
B) Для защиты канала связи путём шифрования трафика
C) Для блокировки вредоносных веб-сайтов
D) Для резервного копирования файлов

4. Как называется атака, при которой злоумышленник внедряет произвольный код в страницу веб-приложения, который затем выполняется в браузере жертвы?

A) SQL-инъекция
B) Cross-Site Request Forgery (CSRF)
C) Cross-Site Scripting (XSS)
D) Переполнение буфера

5. Что из перечисленного является основным назначением межсетевого экрана?

A) Обнаружение вирусов на файловом сервере
B) Шифрование данных на диске
C) Фильтрация сетевого трафика на основе заданных правил
D) Создание резервных копий данных

6. Какой протокол используется для обеспечения безопасной аутентификации и выдачи билетов в домене Windows?

A) RADIUS

B) Kerberos
C) PAP
D) CHAP

7. Какой из перечисленных методов НЕ является фактором многофакторной аутентификации?
A) Пароль (что вы знаете)
B) Сканер отпечатка пальца (что вы есть)
C) SMS-код на телефон (что вы имеете)
D) CAPTCHA-тест (подтверждение, что вы не робот)

8. Что такое DLP-система?
A) Средство обнаружения сетевых атак
B) Комплекс для предотвращения утечек конфиденциальных данных
C) Программа для шифрования баз данных
D) Антивирус с поведенческим анализом

9. Как называется уязвимость, возникающая при недостаточной фильтрации вводимых пользователем данных, что позволяет злоумышленнику изменять структуру SQL-запроса?
A) Command Injection
B) LDAP Injection
C) SQL Injection
D) XPath Injection

10. Какой закон Российской Федерации является основным в сфере регулирования обработки персональных данных?
A) ФЗ «О безопасности критической информационной инфраструктуры» (ФЗ-187)
B) ФЗ «Об информации, информационных технологиях и о защите информации» (ФЗ-149)
C) ФЗ «О персональных данных» (ФЗ-152)
D) ФЗ «Об электронной подписи» (ФЗ-63)

Задания и вопросы для текущего контроля знаний обучающихся по разделам (темам) учебной дисциплины

Тема 1. Введение в кибербезопасность.

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

1. Дайте определение понятию «кибербезопасность». Чем она отличается от информационной безопасности в широком смысле?

2. Перечислите и кратко охарактеризуйте три основных свойства информационной безопасности (триада CIA). Приведите по одному примеру угрозы для каждого свойства.

3. Что такое «уязвимость», «угроза» и «риск»? Как эти понятия связаны между собой?

4. Какие основные виды угроз информационной безопасности вы знаете? Приведите классификацию по источнику возникновения (природные, техногенные, антропогенные).

5. Что такое «модель нарушителя»? Для чего она разрабатывается и какие характеристики нарушителя обычно в неё включают?

6. Назовите основные нормативно-правовые акты Российской Федерации в сфере кибербезопасности. Какой закон регулирует обработку персональных данных?

7. Чем отличаются внешние и внутренние угрозы информационной безопасности? Приведите примеры каждого типа.

8. Что понимается под «социальной инженерией» в контексте кибербезопасности? Приведите 2–3 примера атак методами социальной инженерии.

9. Какие каналы утечки информации существуют? Назовите не менее трёх основных каналов.

10. Что такое «политика информационной безопасности»? Какие разделы обязательно должны присутствовать в политике организации?

Тема 2. Криптографические методы защиты информации

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

1. Чем отличается симметричное шифрование от асимметричного? Назовите преимущества и недостатки каждого подхода.

2. Какие алгоритмы относятся к симметричному шифрованию? Кратко опишите принцип работы AES.

3. Объясните назначение хеш-функций. Назовите два распространённых алгоритма хеширования и их основные свойства (необратимость, устойчивость к коллизиям).

4. Что такое электронная подпись (ЭП)? Из каких этапов состоит процесс создания и проверки ЭП?

5. Для чего нужны протоколы SSL/TLS? Как криптография применяется для защиты веб-трафика?

6. В чём заключается проблема распределения ключей в симметричной криптографии? Как алгоритм Диффи – Хеллмана помогает её решить?

7. Что такое «инфраструктура открытых ключей» (PKI)? Какие компоненты входят в PKI и какова роль удостоверяющего центра?

8. Назовите режимы шифрования блочных алгоритмов (например, ECB, CBC). Какой режим считается уязвимым и почему?

9. Чем отличается алгоритм RSA от ECC? Какой из них обеспечивает ту же стойкость при меньшей длине ключа?

10. Что такое «квантово-устойчивая криптография»? Какие угрозы несут квантовые компьютеры для современных криптоалгоритмов?

Тема 3. Управление доступом и идентификация

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

1. Дайте определения понятиям «идентификация», «аутентификация» и «авторизация». В каком порядке они выполняются при доступе пользователя к системе?

2. Какие существуют факторы аутентификации? Приведите примеры для каждого фактора (знание, владение, наследование).

3. В чём различие между мандатным, дискреционным и ролевым управлением доступом? Приведите примеры систем, использующих каждую модель.

4. Что такое модель Белла – Лападулы? Какие правила доступа она устанавливает и для каких систем предназначена?

5. Что такое многофакторная аутентификация? Приведите пример двухфакторной аутентификации, используемой в реальных сервисах.

6. Как работает протокол Kerberos? Назовите его основные компоненты (клиент, сервер аутентификации, сервер выдачи билетов) и назначение билетов.

7. Какие недостатки присущи парольной аутентификации? Перечислите не менее трёх способов повышения надёжности паролей.

8. Что такое биометрическая аутентификация? Назовите два преимущества и два недостатка биометрии по сравнению с паролями.

9. Какие модели управления доступом применяются в операционных системах семейства Linux? Поясните, как назначаются права на файл для владельца, группы и других пользователей.

10. Что такое SSO и для чего используется протокол SAML? Приведите пример ситуации, где SSO повышает удобство и безопасность.

Тема 4. Сетевая безопасность

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

1. Назовите основные уровни модели OSI, на которых обеспечивается сетевая безопасность. Какие протоколы отвечают за безопасность на сетевом и транспортном уровнях?

2. Что такое межсетевой экран (firewall)? Чем отличаются фильтрующие межсетевые экраны от прокси-серверов и NGFW (Next Generation Firewall)?

3. Как работает система обнаружения вторжений и чем она отличается от системы предотвращения вторжений? Приведите примеры срабатывания каждой из них.

4. Какие уязвимости присущи протоколу ARP? Что такое ARP-spoofing и как от него защититься?

5. Для чего используется технология VLAN в контексте сетевой безопасности? Каким образом можно осуществить VLAN hopping?

6. Объясните принцип работы технологии VPN. Какие протоколы наиболее распространены и в чем их различия?

7. Что такое DDoS-атака? Назовите типы DDoS-атак и способы защиты от них.

8. Как работает протокол SSL/TLS при установлении защищённого соединения? Что такое «рукопожатие» и сертификат сервера?

9. Какие угрозы существуют для беспроводных сетей Wi-Fi? Какие протоколы шифрования считаются устаревшими или безопасными?

10. Что такое DMZ в сетевой архитектуре? Для каких целей она используется и как настраиваются правила межсетевого экрана для доступа из DMZ во внутреннюю сеть?

Тема 5. Безопасность приложений и веб-безопасность

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

1. Назовите основные категории уязвимостей веб-приложений согласно OWASP Top 10. Какие три уязвимости традиционно входят в первую пятёрку?

2. Что такое SQL-инъекция? Какой механизм защиты считается наиболее надёжным и почему?

3. Объясните суть XSS-атаки. Чем отличаются отражённый, сохранённый и DOM-тип XSS?

4. Что такое CSRF? Приведите пример атаки и опишите методы защиты.

5. Какие угрозы связаны с неправильной аутентификацией и управлением сессиями? Как следует хранить пароли в базе данных?

6. Что такое переполнение буфера? Какие меры защиты применяются на уровне компилятора и на уровне разработки?

7. Какие методы анализа безопасности приложений существуют? В чём разница между SAST и DAST?

8. Что такое безопасная конфигурация веб-сервера? Какие заголовки HTTP повышают безопасность?

9. Как работает уязвимость XXE? На каких технологиях она возможна и как от неё защититься?

3 Тестирование по результатам освоения лекционного материала и самостоятельной работы

Тестирование проводится для определения степени усвоения материалов лекций, а также выполнения самостоятельной работы в рамках часов, отведенных на самостоятельную работу обучающихся, в СУО
СибГИУ.

Тема 1. Введение в кибербезопасность.

Перечень вопросов для тестирования:

1. Что такое кибербезопасность?

а) Защита компьютерных сетей и данных от несанкционированного доступа, атак и повреждений

б) Совокупность антивирусных программ

в) Метод шифрования электронной почты

г) Способ резервного копирования файлов

2. Что из перечисленного входит в триаду CIA?

а) Конфиденциальность, Целостность, Доступность

б) Конфиденциальность, Неотказуемость, Аутентичность

в) Целостность, Доступность, Наблюдаемость

г) Доступность, Анонимность, Достоверность

3. Как называется свойство информации, означающее, что доступ к ней разрешён только авторизованным пользователям?

4. К внутренним угрозам информационной безопасности относятся:

а) Атаки хакеров из внешней сети

б) Сбои в работе оборудования по вине производителя

в) Несанкционированные действия сотрудников организации

г) Природные пожары и наводнения

5. Что такое фишинг?

а) Вид компьютерной игры

б) Метод кражи персональных данных через поддельные сайты или письма

в) Программа для защиты от вирусов

г) Система резервного копирования

6. Какой федеральный закон Российской Федерации является основным в сфере защиты персональных данных?

7. Что понимается под «угрозой информационной безопасности»?

а) Совокупность средств защиты информации

б) Совокупность условий и факторов, создающих опасность нарушения защищённости информации

в) Программная уязвимость, позволяющая получить несанкционированный доступ

г) Процесс шифрования данных при передаче

8. Какое понятие описывает величину возможного ущерба от реализации угрозы с учётом вероятности её возникновения?

9. Какие действия помогают защитить данные в интернете?

а) Использование сложных паролей

б) Регулярное обновление программ

в) Включение двухфакторной аутентификации

г) Все перечисленные действия

10. Установите соответствие между термином и его определением:

1. Социальная инженерия

2. Брандмауэр

3. DDoS-атака

А. Программа или устройство, фильтрующее сетевой трафик

Б. Метод психологического воздействия на человека с целью получения конфиденциальной информации

В. Создание множества ложных запросов к серверу для нарушения его работы

Тема 2. Криптографические методы защиты информации

Перечень вопросов для тестирования:

1. В чём основное различие между симметричным и асимметричным шифрованием?

а) В симметричном шифровании используется один ключ, в асимметричном – пара ключей

б) Симметричное шифрование быстрее, но менее надёжно

в) Асимметричное шифрование не требует обмена ключами

г) Все перечисленные варианты верны

2. Какой алгоритм относится к симметричному шифрованию?

3. Что такое хеш-функция?

а) Функция, преобразующая входные данные произвольной длины в выходную строку фиксированной длины

б) Способ шифрования, при котором ключ шифрования и расшифрования совпадают

в) Метод аутентификации пользователя

г) Протокол безопасной передачи файлов

4. Для чего используется электронная подпись?
а) Для шифрования сообщения
б) Для подтверждения авторства и целостности документа
в) Для сжатия данных
г) Для создания резервной копии

5. Какой из перечисленных алгоритмов является алгоритмом хеширования?
а) DES
б) SHA-256
в) RSA
г) Diffie-Hellman

6. Что такое инфраструктура открытых ключей?
а) Система для генерации случайных чисел
б) Комплекс компонентов, обеспечивающих создание, распространение и проверку цифровых сертификатов
в) Набор алгоритмов симметричного шифрования
г) Программа для взлома паролей

7. Какой протокол использует криптографию для защиты соединения между веб-браузером и сервером?

8. Какая длина ключа в алгоритме AES считается достаточной для защиты информации уровня «секретно» согласно современным стандартам?

9. Какие из перечисленных мер повышают безопасность криптосистемы?
а) Регулярная смена ключей
б) Использование сертифицированных алгоритмов
в) Защита закрытых ключей от несанкционированного доступа
г) Все перечисленные меры

10. Установите соответствие между алгоритмом и его типом:
1. RSA
2. MD5
3. AES
А. Хеш-функция
Б. Симметричное шифрование
В. Асимметричное шифрование

Тема 3. Управление доступом и идентификация
Перечень вопросов для тестирования:

1. В каком порядке выполняются идентификация, аутентификация и авторизация при доступе пользователя к системе?

а) Аутентификация → Идентификация → Авторизация

б) Идентификация → Аутентификация → Авторизация

в) Авторизация → Идентификация → Аутентификация

г) Идентификация → Авторизация → Аутентификация

2. Что из перечисленного относится к фактору аутентификации «то, чем вы являетесь»?

а) Пароль

б) Смарт-карта

в) Отпечаток пальца

г) SMS-код

3. В чём заключается различие между дискреционным и мандатным управлением доступом?

а) Дискреционное управление доступом основано на ролях пользователей, а мандатное – на метках конфиденциальности

б) Дискреционное позволяет владельцу ресурса самому назначать права, а мандатное использует глобальные метки безопасности

в) Дискреционное управление доступом не требует аутентификации

г) Мандатное управление доступом используется только в Linux

4. Какой протокол аутентификации является основным в домене Windows и использует билеты?

5. Что такое двухфакторная аутентификация?

а) Использование двух разных паролей

б) Использование двух различных факторов аутентификации

в) Двукратный ввод одного пароля

г) Использование двух разных логинов

6. Какая модель управления доступом применяется в операционной системе Linux при использовании команд chmod?

7. Что такое биометрическая аутентификация?

а) Аутентификация с помощью пароля, сгенерированного случайным образом

б) Аутентификация на основе уникальных физических характеристик человека

в) Аутентификация с помощью SMS-кода

г) Аутентификация с использованием токенов

8. Какая модель управления доступом предполагает назначение прав в зависимости от должностных обязанностей пользователя?

9. Какие из перечисленных мер повышают надёжность аутентификации?

а) Использование сложных паролей

б) Введение задержки после нескольких неудачных попыток входа

в) Применение многофакторной аутентификации

г) Все перечисленные меры

10. Установите соответствие между термином и его определением:

1. Идентификация

2. Аутентификация

3. Авторизация

А. Проверка подлинности пользователя

Б. Процесс сопоставления субъекта доступа с его уникальным признаком

В. Определение разрешённых действий пользователя после успешной аутентификации

Тема 4. Сетевая безопасность

Перечень вопросов для тестирования:

1. Что такое межсетевой экран?

а) Устройство или программа, фильтрующие сетевой трафик на основе заданных правил

б) Программа для шифрования файлов

в) Специализированный сервер для хранения паролей

г) Антивирус, проверяющий входящие письма

2. В чём основное отличие системы обнаружения вторжений (IDS) от системы предотвращения вторжений?

3. Какой протокол используется для создания защищённых VPN-соединений на транспортном уровне?

4. Что такое DDoS-атака?

а) Атака с целью подбора пароля

б) Атака, направленная на нарушение доступности сервиса путём большого количества ложных запросов

в) Атака с внедрением вредоносного кода в веб-страницу

г) Атака с перехватом сетевого трафика

5. Для чего используется технология VLAN?

а) Для увеличения пропускной способности сети

б) Для логического разделения сети на изолированные сегменты

в) Для беспроводного доступа
г) Для резервного копирования данных

6. Что такое ARP-spoofing (отравление ARP)?
а) Атака, при которой злоумышленник подменяет ARP-ответы, чтобы перенаправить трафик на свой узел
б) Метод шифрования ARP-запросов
в) Способ настройки маршрутизации
г) Протокол безопасной передачи ARP-пакетов

7. Какой протокол обеспечивает защищённое соединение между веб-браузером и сервером?

8. Что такое DMZ (демилитаризованная зона) в сетевой архитектуре?

9. Какие из перечисленных мер повышают безопасность беспроводной сети Wi-Fi?
а) Использование протокола WPA2 или WPA3
б) Отключение функции WPS
в) Скрытие SSID сети
г) Все перечисленные меры

10. Установите соответствие между типом атаки и её описанием:
1. Sniffing
2. Spoofing
3. Man-in-the-Middle
А. Злоумышленник выдает себя за легитимное устройство или пользователя
Б. Прослушивание сетевого трафика с целью захвата данных
В. Злоумышленник встраивается в канал связи между двумя сторонами

Тема 5. Безопасность приложений и веб-безопасность
Перечень вопросов для тестирования:
1. Что такое SQL-инъекция?
а) Внедрение вредоносного кода в SQL-запрос через нефильтрованные пользовательские данные
б) Атака, направленная на подбор пароля к базе данных
в) Метод шифрования данных в SQL
г) Способ резервного копирования баз данных

2. Какой тип XSS-атаки сохраняется на сервере и выполняется у всех пользователей, открывающих страницу?
3. Что такое CSRF?

а) Атака, при которой злоумышленник заставляет браузер жертвы выполнить нежелательное действие на доверенном сайте

б) Атака на криптографические ключи

в) Уязвимость веб-сервера, позволяющая просматривать системные файлы

г) Метод взлома SSL/TLS

4. Какая из перечисленных мер является наиболее эффективной защитой от SQL-инъекций?

а) Экранирование кавычек

б) Использование параметризованных запросов

в) Скрытие текста ошибок базы данных

г) Использование сложных паролей

5. Что из перечисленного относится к уязвимостям аутентификации и управления сессиями?

а) Хранение паролей в открытом виде в базе данных

б) Использование предсказуемых идентификаторов сессии

в) Отсутствие защиты от автоматического подбора паролей

г) Все перечисленные варианты

6. Что такое переполнение буфера?

а) Ошибка, возникающая при записи данных за границы выделенного буфера в памяти

б) Переполнение очереди запросов к веб-серверу

в) Превышение лимита трафика

г) Ошибка в работе сетевого протокола

7. Для чего используется заголовок HTTP Content-Security-Policy?

а) Для указания браузеру, какие источники ресурсов разрешены для загрузки

б) Для сжатия контента

в) Для шифрования ответа сервера

г) Для кэширования страниц

8. Что такое SAST?

9. Какие из перечисленных принципов относятся к безопасному программированию?

а) Никогда не доверять пользовательскому вводу

б) Использовать принцип наименьших привилегий

в) Не выводить подробные ошибки пользователю

г) Все перечисленные принципы

10. Установите соответствие между уязвимостью и её описанием:

1. XSS

2. CSRF
3. SQL Injection
А. Внедрение вредоносного кода в запрос к базе данных
Б. Выполнение вредоносного сценария в браузере жертвы
В. Принудительное выполнение нежелательного действия от имени аутентифицированного пользователя

4 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.