

АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.05.01 Методы и средства защиты информации

Направление подготовки бакалавриата

09.03.02 «Информационные системы и технологии»

Направленность (профиль подготовки)

«Информационные системы и технологии»

1.	<p>Цель изучения дисциплины</p> <p>Целями освоения дисциплины Б1.В.ДВ.05.01 «Методы и средства защиты информации» являются формирование у студентов компетенций в области информационной безопасности и применения на практике методов и средств защиты информации</p>		
2.	<p>Место дисциплины в структуре ОПОП ВО бакалавриата</p> <p>Дисциплина «Методы и средства защиты информации» относится к базовой части Б1. Освоение дисциплины основывается на знаниях студентов, полученных ими в ходе изучения дисциплин предыдущих курсов: «Интеллектуальные информационные системы и технологии», «Архитектура информационных систем», «Теория информационных процессов и систем». Данная дисциплина необходима для освоения следующих дисциплин: «Инструментальные средства информационных систем», «Методы и средства проектирования информационных систем и технологий».</p>		
3.	<p>Результаты освоения дисциплины (модуля) <u>Б1.В.ДВ.05.01 «Методы и средства защиты информации»</u></p>		
	Код и наименование компетенции	Индикаторы	Дескрипторы
	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1.: понимает виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность. УК-2.2.: проводит анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности.	Знать: виды ресурсов ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность. Уметь: проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно правовую документацию в сфере профессиональной деятельности.
	Профессиональные компетенции (ПК)		

<p>ПК-4. Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности</p>	<p>ПК-4.1: использует специальные знания по работе с установленной БД; общие основы решения практических задач по восстановлению БД и проверке корректности восстановленных данных; основы управления учетными записями пользователей;</p> <p>ПК-4.2: выполняет регламентные процедуры по резервированию данных; выбирать способ действия из известных; контролировать оценивать и корректировать свои действия; выполнять регламентные процедуры по восстановлению и проверке корректности восстановленных данных; выбирать способ действия из известных; контролировать оценивать и корректировать свои действия; применять специальные процедуры управления правами доступа пользователей</p> <p>ПК-4.3: запускает процедуры резервного копирования; мониторинга выполнения процедуры резервного копирования; контроля завершения процедуры резервного копирования; запуска процедуры восстановления БД; мониторинга выполнения процедуры восстановления БД; контроля завершения процедуры восстановления БД; назначения прав доступа пользователей к БД изменения прав доступа пользователей к БД; контроля соблюдения прав доступа пользователей к БД.</p>	<p>Знать: специальные знания по работе с установленной БД;</p> <p>общие основы решения практических задач по восстановлению БД и проверке корректности восстановленных данных; специальные знания по работе с установленной БД основы управления учетными записями пользователей; специальные знания по работам с установленной БД.</p> <p>, Уметь: выполнять регламентные процедуры по резервированию данных; выбирать способ действия и известных; контролировать оценивать и корректировать свои действия; выполнять регламентные процедуры по восстановлению и проверки корректности восстановленных данных; выбирать способ действия из известных контролировать, оценивать корректировать свои действия применять специальные процедуры управления правами доступа пользователей;</p> <p>Владеть навыками: запуск процедуры резервного копирования; мониторинг выполнения процедуры резервного копирования; контроля завершения; процедуры резервного копирования; запуска процедуры восстановления БД мониторинга выполнения процедуры восстановления БД контроля завершения процедуры восстановления БД назначения прав доступа пользователей к БД; изменений прав доступа пользователей к БД</p>
<p>Профессиональные компетенции (ПК)</p>		

	<p>ПК-8. Способность выполнять работы по разработке компонентов системных программных продуктов: компилятор, загрузчиков, сборщиков, системных утилит, драйверов устройств, по созданию инструментальных средств программирования</p>	<p>ПК-8.1.: понимает синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования; методологии разработки программного обеспечения; методологии и технологии проектирования и использования баз данных; технологии программирования; особенности выбранной среды программирования и системы управления базами данных; компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними;</p> <p>ПК-8.2: применяет выбранные языки программирования для написания программного кода; использовать выбранную среду программирования и средства системы управления базами данных; использовать возможности имеющейся технической и/или программной архитектуры;</p>	<p>Знать: синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования; методологии разработки программного обеспечения; методологии и технологии проектирования и использования баз данных; технологии программирования; особенности выбранной среды программирования и системы управления базами данных; компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними; Уметь: применять выбранные языки программирования для написания программного кода; использовать выбранную среду программирования и средства системы управления базами данных; использовать возможности имеющейся технической и/или программной архитектуры</p>
--	--	---	---

4.	Структура и содержание дисциплины				
	4.1. Структура дисциплины				
	Вид учебной работы	Всего	Порядковый номер семестра		
			5		
	Общая трудоемкость дисциплины всего (в з.е.), в том числе:	5			
	Курсовой проект (работа)	-			
	Аудиторные занятия всего (в акад. часах), в том числе:	68			
	Лекции	36			
	Практические занятия, семинары	-	-		
	Лабораторные работы	32			
	Самостоятельная работа всего (в акад. часах), в том числе:	85			
	КСР	-	-		
	Экзамен	27	-	27	
	Общая трудоемкость дисциплины	180ч.			
4.2. Содержание дисциплины					

Тема 1. Понятие и сущность информационной безопасности и защиты информации. Необходимость и значимость нормативно-правового определения основных понятий. Понятие информационной безопасности (ИБ) и защиты информации. Основные компоненты безопасности государства и доминирующая роль ИБ. Становление и развитие понятия «информационная безопасность». Связь ИБ с информатизацией общества. Базовые уровни обеспечения ИБ и защиты информации.

Тема 2. Основные угрозы информационной безопасности. Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз.

Тема 3. Правовой уровень обеспечения информационной безопасности. Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере ИБ и защиты информации. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне. Степени конфиденциальности сведений, составляющих коммерческую тайну. Методика формирования на фирме перечня сведений, относящихся к коммерческой тайне.

Тема 4. Административный уровень обеспечения информационной безопасности. Концепция ИБ, её цели и этапы построения. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику безопасности, и основные этапы разработки политики ИБ. Задачи, решаемые при анализе рисков для ИС. Базовые методики, используемые для оценки рисков. Основные стандарты в области разработки ПИБ и анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации ПИБ

Тема 5. Программно-технический уровень обеспечения защиты информации. Программные сервисы защиты информации в ИС. Идентификация и аутентификация пользователей как передовой рубеж защиты информации. Базовые методы парольной аутентификации. Модели разграничения доступа к информации. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности. Базовые методы криптографического преобразования данных. Потокковое и блочное шифрование. Процедура формирования электронной подписи. Экранирование информации в информационно-телекоммуникационных сетях (ИТС). Основные сервисы защиты в ИТС. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними.

Антивирусные программные комплексы.

Тема 6. Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня Управление персоналом Физическая защита Поддержание работоспособности Реагирование на нарушения режима безопасности Планирование восстановительных работ.

Тема 7. Система защиты информации. Процесс развития средств и методов защиты информации Этапы развития системы защи-

ты информации в настоящее время Комплексный подход к построению системы защиты информации Системный подход к построению системы защиты информации Цели задачи системы защиты информации. Этапы и порядок проведения работ по созданию системы защиты информации. Структура систем защиты информации на современном этапе. Методы (виды) обеспечения защиты информации.

Тема 8. Обеспечение режима конфиденциальности при работе с защищаемой информацией.

Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиденциальным сведениям, документам и базам данных Допуск должностных лиц, работников к конфиденциальной информации Доступ должностных лиц, работников к конфиденциальным сведениям, документам и базам данных Обязанности должностных лиц, допущенных к сведениям, составляющим коммерческую тайну Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям

Тема 9. Контроль за соблюдением требований информационной безопасности и защиты информации.

Основные положения по осуществлению контроля, назначение, цель и задачи контроля. Основные мероприятия по осуществлению контроля. Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа Проведение служебного расследования по фактам утечки конфиденциальной информации, утраты носителей, содержащих такие сведения, а также по фактам грубых нарушений режима конфиденциальности.

Тема 10. Ответственность за правонарушения информационной безопасности и защиты информации.

Понятие и виды юридической ответственности за нарушение правовых норм по защите информации Меры дисциплинарной ответственности согласно Трудового кодекса РФ Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности Уголовная ответственность за правонарушения в области защиты государственной тайны Уголовная ответственность за правонарушения в области конфиденциальной информации.

Тема 11. Анализ угроз. Проблемы безопасности IP-сетей. Пути решения проблем защиты информации в сетях. Политика безопасности.

Рост популярности Интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т. д. . В ближайшем будущем их число во много раз возрастет, поэтому вероятность доступа хакеров к уязвимым компьютерам и компьютерным сетям также постоянно возрастает. На практике IP-сети уязвимы для многих способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий (например, с появлением мобильных Java-приложений и элементов ActiveX) список возможных типов сетевых атак на IP-сети постоянно расширяется.

Тема 12. Международные стандарты безопасности. Стандарты информационной безопасности в Интернете. Отечественные стандарты безопасности информационных технологий.

В последнее время в мире бурно развивается электронная коммерция посредством сети Интернет. Развитие электронной коммерции в основном определяется прогрессом в области безопасности информации. При этом базовыми задачами являются обеспечение доступности, конфиденциальности, целостности и юридической значимости информации. По оценке Комитета ООН по предупреждению преступности и борьбе с ней, компьютерная преступность вышла на уровень одной из международных проблем. Поэтому чрезвычай-

5.	<p>чайно важно добиваться эффективного решения проблем обеспечения безопасности коммерческой информации в глобальной сети Интернет и смежных intranet-сетях, которые по своей технической сущности не имеют принципиальных отличий и различаются в основном масштабами и открытостью.</p> <p>Тема 13. Симметричные криптосистемы. Блочные шифры. Конструкция Фейстеля. Режимы шифрования блочных шифров. Стандарты блочного шифрования. Стандарт России - ГОСТ 28147-89. Поточные шифры. Шифр RC4..</p> <p>Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.</p> <p>Обмен информацией осуществляется в 3 этапа:</p> <ol style="list-style-type: none"> 1. отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар); 2. отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю; 3. получатель получает сообщение и расшифровывает его. <p>Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.</p> <p>Тема 14. Введение в теорию чисел. Метод распределения ключей Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамала. Стандарты России ГОСТ 34.10, ГОСТ 34.11</p> <p>Криптосистемы Диффи-Хеллмана и Эль-Гамала основаны на вычислительной сложности задачи дискретного логарифмирования. Вычисление $y = ax \pmod{p}$ (p – простое число или степень простого числа, $1 < x < p-1$, $1 < a < p-1$, $1 < b < p-1$, $ac = b \pmod{p}$) выполняется просто, но вычисление $x = \log_a y \pmod{p}$ выполняется достаточно сложно. Алгоритм Диффи-Хеллмана предназначен только для генерации ключа симметричного шифрования, который затем будет использован субъектами А и В для защищенного обмена сообщениями по открытой сети.</p> <p>Тема 15. Простая аутентификация. Строгая аутентификация. Биометрическая аутентификация.</p> <p>Процедура проверки подлинности. Она может быть односторонней или взаимной, обычно проводится с помощью криптографических способов. Не следует путать с авторизацией (процедурой предоставления субъекту определенных прав) и идентификацией (процедурой распознавания субъекта по его идентификатору)</p> <p>Тема 16. Обеспечение безопасности ОС. Технологии межсетевых экранов.</p> <p>Сетевые атаки несут с собой большую опасность для корпоративных сетей и домашних пользователей. Для их предотвращения, обнаружения и блокирования человечество придумало разнообразные механизмы и средства, их реализующие. Однако надо понимать, что невозможно рассмотреть все до единого механизмы и все аспекты, связанные с разнообразными средствами защиты.</p>
	Образовательные технологии

	<p>При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:</p> <p>1. Internet - технологии:</p> <p>WWW(англ. WorldWideWeb- Всемирная Паутина) - технология работы в сети с гипертекстами;</p> <p>FTP(англ. FileTransferProtocol- протокол передачи файлов) - технология передачи по сети файлов произвольного формата;</p> <p>IRC(англ. InternetRelayChat- поочередный разговор в сети, чат) - технология ведения переговоров в реальном масштабе времени, дающая возможность разговаривать с другими людьми по сети в режиме прямого диалога;</p> <p>ICQ(англ. Iseekyou- я ищу тебя, можно записать тремя указанными буквами) - технология ведения переговоров один на один в синхронном режиме.</p> <p>2. Дистанционное обучение с использованием ЭИОС на платформе Moodle.</p> <p>3. Технология мультимедиа в режиме диалога.</p> <p>4. Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории).</p> <p>5. Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии) и т.д.</p>
6.	<p>Используемые ресурсы информационно-телекоммуникационной сети «Internet»; информационные технологии, программные средства и информационно-справочные системы</p> <p>1. Электронная информационно-образовательная среда АНО ВО "СЗТУ" (ЭИОС СЗТУ) [Электронный ресурс]. - Режим доступа: http://edu.nwotu.ru/</p> <p>2. Учебно-информационный центр АНО ВО "СЗТУ" [Электронный ресурс]. - Режим доступа: http://lib.nwotu.ru:8087/jirbis2/</p> <p>3. Электронно-библиотечная система IPRbooks [Электронный ресурс]. - Режим доступа: http://www.iprbookshop.ru/</p> <p>4. Информационная система "Единое окно доступа к образовательным ресурсам" [Электронный ресурс]. - Режим доступа: http://window.edu.ru/</p> <p>5. Информационная системы доступа к электронным каталогам библиотек сферы образования и науки (ИС ЭКБСОН) [Электронный ресурс]. - Режим доступа: http://www.vlibrary.ru/</p> <p>Программное обеспечение</p> <p>При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:</p> <p>Internet- технологии:</p> <p>WWW(англ. WorldWideWeb- Всемирная Паутина) - технология работы в сети с гипертекстами;</p> <p>FTP(англ. FileTransferProtocol- протокол передачи файлов) - технология передачи по сети файлов произвольного формата;</p> <p>IRC(англ. InternetRelayChat- поочередный разговор в сети, чат) - технология ведения переговоров в реальном масштабе времени, дающая возможность разговаривать с другими людьми по сети в режиме прямого диалога;</p> <p>ICQ(англ. Iseekyou- я ищу тебя, можно записать тремя указанными буквами) - технология ведения переговоров один на один в синхронном режиме.</p> <p>Дистанционное обучение с использованием ЭИОС на платформе Moodle.</p> <p>Технология мультимедиа в режиме диалога.</p>

	<p>Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории).</p> <p>Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии) и т.д.</p> <p>Программное обеспечение: ППП MSOffice2010</p>
7.	Формы текущего контроля
	<ul style="list-style-type: none"> • Коллоквиум; • Тест; • Контрольная работа; • Отчеты студентов по лабораторным работам.
8.	Форма промежуточного контроля
	Экзамен

Разработчик: старший преподаватель кафедры ИСиТ Цуроев И. М.