Приложение
к рабочей программе модуля (дисциплины)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Код модуля	Модуль
1156042	*Криптографические методы защиты информации*

Екатеринбург, 2021

Оценочные материалы по модулю составлены авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*
2	Пономарева Ольга Алексеевна		Старший преподаватель	*Учебно-научный центр «Информационная безопасность»*

Согласовано:

Управление образовательных программ Р.Х.Токарева

1. **СТРУКТУРА И ОБЪЕМ МОДУЛЯ** *Управление информационной безопасностью информационных систем персональных данных (ИСПДн), государственных информационных систем (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)*

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах	Форма итоговой промежуточной аттестации по дисциплинам модуля и в целом по модулю
1.	Криптографические алгоритмы и протоколы	*3/108*	*3*
2	Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ	*3/108*	З
	ИТОГО по модулю:	***6/216***	

2. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО МОДУЛЮ

2.1. Проект по модулю

Не предусмотрено

2.2. Интегрированный экзамен по модулю

Не предусмотрено

Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 1

Модуль *Криптографические методы защиты информации*

Дисциплина Криптографические алгоритмы и протоколы

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Чадов Антон Юрьевич,		старший преподаватель кафедры защиты информации	МИФИ

~~1.~~ ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ *Защита информации в системах беспроводной связи*

Таблица 1

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	З-1 - знать основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов. З-2 - знать правила создания технического задания на создание подсистем безопасности информационных систем. З-3 - знать основные угрозы безопасности информации и модели нарушителя в информационных системах. З-4 - знать основные нормативные правовые акты в области обеспечения информационной безопасности. З-5 - знать нормативные методические документы ФСБ России в области защиты информации. З-6 - знать нормативные методические документы ФСТЭК России в области информационной безопасности. У-1 - уметь разрабатывать технические задания на создание подсистем обеспечения информационной безопасности. У-2 - уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности. У-3 - уметь разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации. У-4 - уметь разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации. У-5 - уметь разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности. У-6 - уметь работать с технической и эксплуатационной документацией. У-6 - уметь оценивать различные инструменты в области проектирования и управления информационной безопасности. П-1 - владеть навыками разработки политик безопасности различных уровней.

	П-2 - владеть навыками расчета и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления рисками информационной безопасности. П-3 - владеть правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации. П-4 - владеть навыками работы с нормативными правовыми актами в области информационной безопасности.

1. **ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ** *Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ*

Таблица 2

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности поставленной цели	*З-1 - знает методы концептуального проектирования технологий обеспечения информационной безопасности.* *З-2 - знает направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем.* *З-3 - знает современные методы и средства тестирования.* *З-4 - знать принципы построения и функционирования современных информационных систем.* *З-5 - знать назначение комплексной системы защиты информации, принципы ее организации и этапы разработки.* *З-6 - знать требования к системам комплексной защиты информации* *У-1 - умеет выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.* *У-2 - умеет разрабатывать тестовые планы и сценарии тестирования разработанного продукта.* *У-3 - умеет управлять коллективом исполнителей и принимать управленческие решения.* *У-4 - уметь проектировать подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов.* *У-5 - уметь разрабатывать модели угроз и нарушителей информационной безопасности информационных систем.*

	П-1 - владеет навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности. *П-2 - владеет навыками практической реализации типовых задач разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.* *П-3 - владеет средствами автоматизированного и ручного функционального тестирования.* *П-4 - владеть навыками участия в организации комплексной системы защиты объекта.*

2. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

2.1. Распределение объема времени по видам учебной работы

Таблица 2

№ п/п	Наименование дисциплины модуля	Объем времени, отведенный на освоение дисциплины модуля								
		Аудиторные занятия, час.				Промежуточная аттестация (форма итогового контроля /час.)	Контактная работа (час.)	Самостоятельная работа студента, включая текущую аттестацию (час.)	Всего по дисциплине	
		Занятия лекционного типа	Практические занятия	Лабораторные работы	Всего				Час.	Зач. ед.
1	2	3	4	5	6	7	8	9	10	11
1.	Криптографические алгоритмы и протоколы	36	-	18	54	Э	62,35	43,57	108	3
Всего на освоение дисциплины модуля (час.)		36		18	54	Э	62,35	43,57	108	3

2.2. Виды СРС, количество и объем времени на контрольно-оценочные мероприятия СРС по дисциплине

Контрольно-оценочные мероприятия СРС включают самостоятельное изучение материала, подготовку к аудиторным занятиям и мероприятиям текущего контроля, выполнение и оформление внеаудиторных мероприятий текущего контроля и подготовку к мероприятиям промежуточного контроля.

Таблица 3

№ п/п	Вид самостоятельной работы студента по дисциплине модуля	Количество контрольно-	Объем контрольно-

		оценочных мероприятий СРС	оценочных мероприятий СРС (час.)
1.	*Подготовка к лекционным*	*6*	*10 час.*
2	*Подготовка к практическим занятиям*	*16*	*16 час.*
3.	*Самостоятельное изучение материала*		*8,57*
	Подготовка к экзамену	1	9 час.
	Итого на СРС по дисциплине:		*43,57 час.*

3. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

3.1 В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Личностные качества	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

3.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)	Шкала оценивания		
		Традиционная характеристика уровня		Качественная характеристика уровня
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

4. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ДИСЦИПЛИНЕ МОДУЛЯ

Зачет в форме итогового тестирования с использованием ОК при реализации модели исключительно электронного обучения с использованием внутреннего онлайн-курса (ОК) УрФУ http://courses.openedu.urfu.ru/courses/course-v1:UrFU+AOVZ+spring_2018/info

Спецификация теста в системе ОК УрФУ:

Для проведения промежуточной аттестации используется ОК УрФУ.

Структура тестовых материалов при использовании ОК УрФУ: Тест включает в себя 40 заданий, время выполнения – 60 минут. В структуре теста представлены вопросы по всем разделам изучения дисциплины.

Перечень типовых (примерных) вопросов текущего контроля знаний

1. Контрольная работа по теме «Криптографические алгоритмы»

1) Криптография это –

а)наука об обеспечении безопасности информации с использованием математических преобразований

б) наука, занимающаяся методами шифрования и расшифровывания

в) наука о методах дешифровки зашифрованной информации без предназначенного для этого ключа, а также сам процесс такой дешифровки.

2) Криптология это –

а)наука об обеспечении безопасности информации с использованием математических преобразований

б) наука, занимающаяся методами шифрования и расшифровывания

в) наука о методах дешифровки зашифрованной информации без предназначенного для этого ключа, а также сам процесс такой дешифровки.

3) Криптоанализ это –

а)наука об обеспечении безопасности информации с использованием математических преобразований

б) наука, занимающаяся методами шифрования и расшифровывания

в) наука о методах дешифровки зашифрованной информации без предназначенного для этого ключа, а также сам процесс такой дешифровки.

4) Криптосистемы с секретным ключом в общем случае

а) быстрее, чем криптосистемы с открытым ключом

б) медленнее, чем криптосистемы с открытым ключом

в) сравнимы по скорости с криптосистемами с открытым ключом

5) Блочный и поточный шифры:

а) оба – симметричные шифры

б) блочный – симметричный, поточный – асимметричный

в) блочный – асимметричный, поточный – симметричный

г) оба – асимметричные шифры

6) Какой из этих методов позволяет надёжно обеспечить конфиденциальность информации:

а) цифровая подпись

б) шифрование

в) хэширование

г) сжатие

7) Какой из этих методов позволяет обеспечить целостность информации:

а) шифрование

б) сжатие

в) цифровая подпись

г) кодирование

7) В схемах шифрования с открытым ключом

а)прямое преобразование выполняется закрытым ключом, а обратное – открытым

б) прямое преобразование выполняется открытым ключом, а обратное – закрытым

в) оба преобразования выполняются закрытым ключом, а открытый при необходимости получается из закрытого

г) оба преобразования выполняются открытым ключом, а закрытый при необходимости получается из открытого

8) В схемах электронной подписи

а)прямое преобразование выполняется закрытым ключом, а обратное – открытым

б) прямое преобразование выполняется открытым ключом, а обратное – закрытым

в) оба преобразования выполняются закрытым ключом, а открытый при необходимости получается из закрытого

г) оба преобразования выполняются открытым ключом, а закрытый при необходимости получается из открытого

9) В системах с открытым ключом

а) открытый ключ можно получить из закрытого

б) закрытый ключ можно получить из открытого

в) ключи независимы и нельзя получить один из другого

г) можно получить как открытый из закрытого, так и наоборот

10) DES – это

а) асимметричный алгоритм

б) симметричный потоковый алгоритм

в) симметричный блочный алгоритм с размером блока 64 бита

г) симметричный блочный алгоритм с размером блока 512 ит

2. Контрольная работа по теме «Введение в криптографические протоколы»

1) Протокол – это

а) упорядоченный набор действий, описанный на материальном носителе

б) конечная совокупность точно заданных правил решения произвольного класса задач или набор инструкций, описывающих порядок действий исполнителя для решения некоторой задачи

в) описание распределённого алгоритма, в процессе выполнения которого два или более участников последовательно выполняют определённые действия и обмениваются сообщениями

2) Защищённым протоколом или протоколом обеспечения безопасности будет называть протокол, обеспечивающий выполнение:

а) аутентификации сторон и источника данных

б) разграничения доступа

в) конфиденциальности,

г) целостности,

д) невозможности отказа от факта отправки или получения

е) все пункты а)-д)

ж) любой из пунктов а)-д)

3) Под атакой на защищённый протокол понимается

а) попытка проведения анализа сообщений протокола и/или выполнениянепредусмотренных протоколом действий для нарушения заявленных или подразумеваемых свойств протокола

б) кража ключа, используемого в протоколе

в) установка на компьютер программы, сохраняющей записывающей ввод данных с клавиатуры

4) Криптографическая стойкость протокола Диффи — Хеллмана основана на сложности задачи:

а) факторизации

б) дискретного логарифмирования

в) матричного преобразования

г) вычисления эллиптической кривой

5) Выберите верное утверждение:

а) протоколы обмена ключами делятся на два типа: протоколы передачи ключа и протоколы совместной выработки ключа

б) протоколы передачи ключа делятся на два типа: протоколы обмена ключами и протоколы совместной выработки ключа

в) протоколы совместной выработки ключа делятся на два типа: протоколы передачи ключа и протоколы обмена ключами

6) Протокол EKE (Encrypted Key Exchange)

а) использует только асимметричную криптографию

б) использует только симметричную криптографию

в) использует как симметричную, так и асимметричную криптографию

г) не использует симметричную и асимметричную криптографию

7) Идентификация — это

а) процедура проверки подлинности

б) процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе

в) предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий

8) Аутентификация — это

а) процедура проверки подлинности

б) процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе

в) предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий

9) Авторизация — это

а) процедура проверки подлинности

б) процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе

в) предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий

10) Многофакторная аутентификация проводится по факторам различной природы, к ним относятся:

а) свойство, которым обладает субъект, например, биометрия, природные уникальные отличия (лицо, радужная оболочка глаз, папиллярные узоры, последовательность ДНК)

б) знание – информация, которую знает субъект, например, пароль, PIN (Personal Identification Number).

в) владение – вещь, которой обладает субъект, например, электронная или магнитная карта, флэш-память

г) состояние – состояние объекта в информационной системе, например, число его открытых сессий или уровень доступа

д) верны варианты а)-в)

е) верны варианты а)-д)

ж) верны несколько вариантов, но не д и е

з) нет верных вариантов

3. Контрольная работа по теме «Протоколы защиты данных в сети Internet и протоколы генерации и распределения ключей»

1) Сетевая модель OSI –

а) Open Security Interfaces

б) Open Systems Interconnection

в) Old System of Internet

2) Сетевая модель OSI состоит из

а) 4 уровней

б) 6 уровней

в) 7 уровней

г) 12 уровней

3) Протокол IP находится на

а) физическом уровне модели OSI

б) транспортном уровне модели OSI

в) сетевом уровне модели OSI

г) сеансовом уровне модели OSI

д) стабильном уровне модели OSI

4) Протокол SSH находится на

а) физическом уровне модели OSI

б) транспортном уровне модели OSI

в) сетевом уровне модели OSI

г) сеансовом уровне модели OSI

д) стабильном уровне модели OSI

5) Протокол SSL использует

а) асимметричную криптографию

б) симметричное шифрование

в) коды аутентификации

г) все пункты а)-в) верны

6) Kerberos – это протокол

а) шифрования

б) подписи

в) идентификации

г) аутентификации

7) К методам противодействия атаке обменом относится:

а) сохранении в тайне от противника информации, определяющей алгоритм идентификации

б) использование различных форматов сообщений, передаваемых на разных шагах протокола

в) вставка в сообщения специальных идентификационных меток и номеров сообщений

г) использование временных меток

д) вставка в передаваемые сообщения случайных чисел

е) варианты а)-в)

ж) варианты г) и д)

з) все варианты

8) К методам противодействия атаке повтором относится:

а) сохранении в тайне от противника информации, определяющей алгоритм идентификации

б) использование различных форматов сообщений, передаваемых на разных шагах протокола

в) вставка в сообщения специальных идентификационных меток и номеров сообщений

г) использование временных меток

д) вставка в передаваемые сообщения случайных чисел

е) варианты а)-в)

ж) варианты г) и д)

з) все варианты

9) К протоколам распределения ключей относится протокол:

а) Нидхема-Шрёдера

б) RSA

в) SSL

г) варианты а)-в)

д) ни один из вышеперечисленных

10) IPSec обычно используется для:

а) организации безопасного доступа к web-сайтам

б) организации защищенного удаленного доступа к системе

в) организации VPN-соединения

4. Контрольная работа по теме «Протоколы генерации и распределения ключей. Протоколы разделения секретов. Протоколы с нулевым разглашением и доказательство нулевого разглашения»

1) Идея пороговой (K,M)-схемы разделения общего секрета среди M пользователей состоит в следующем. Доверенная сторона хочет распределить некий секрет K0 между M пользователями таким образом, что:

а) любые $m1$: $K<=m1<=N$, легальных пользователей могут получить секрет (или доступ к секрету), если предъявят свои секретные ключи;

б) любые$m2$:$m2<K$, легальных пользователей не могут получить секрет и не могут определить (вычислить) этот секрет, даже решив трудную в вычислительном смысле задачу

в) оба варианта а) и б) верны

г) оба варианта а) и б) верны, но не хватает дополнительного условия

2) Схема разделения секрета Блэкли основывается на том, что

а) для восстановления всех координат точки в -мерном пространстве, принадлежащей нескольким неколлинеарным гиперплоскостям, необходимо и достаточно знать уравненияK таких плоскостей

б) основывается на том, что для восстановления всех коэффициентов полинома$P(x)$ =$aK-1xK-1+\cdots+a1x+a0$степени$K-1$требуетсяKкоординат различных точек, принадлежащих кривой $y=P(x)$. Все операции проводятся в конечном поле$GF(p)$.

в) основывается на лежащей в основе RSA задаче факторизации

г) варианты а) и б)

д) варианты а)-в)

3) Схема разделения секрета Шамир основывается на том, что

а) для восстановления всех координат точки в -мерном пространстве, принадлежащей нескольким неколлинеарным гиперплоскостям, необходимо и достаточно знать уравнения K таких плоскостей

б) основывается на том, что для восстановления всех коэффициентов полинома $P(x) = aK-1xK-1+\cdots+a1x+a0$ степени$K-1$ требуется K координат различных точек, принадлежащих кривой $y=P(x)$. Все операции проводятся в конечном поле $GF(p)$.

в) основывается на лежащей в основе RSA задаче факторизации

г) варианты а) и б)

д) варианты а)-в)

4) Схема разделения секрета Брикелла – это

а) Пороговая схема

б) Схема разделения секрета по коалициям

5) Доказательство с нулевым разглашением — это

а) интерактивный вероятностный протокол, который позволяет доказать, что доказываемое утверждение верно, и Доказывающий знает это доказательство, в то же время, не предоставляя никакой информации о самом доказательстве данного утверждения.

б) интерактивный вероятностный протокол, который позволяет доказать, что доказываемое утверждение верно ещё на нулевой итерации

в) интерактивный вероятностный протокол, который позволяет доказать, что доказываемое утверждение верно, не разглашая никакой информации третьим лицам

6) Доказательство с нулевым разглашением должно обладать следующим свойством:

а) полнота: если утверждение действительно верно, то Доказывающий убедит в этом Проверяющего с любой наперед заданной точностью

б) корректность: если утверждение неверно, то любой, даже «нечестный», Доказывающий не сможет убедить Проверяющего за исключением пренебрежимо малой вероятности

в) нулевое разглашение: если утверждение верно, то любой, даже «нечестный», Проверяющий не узнает ничего кроме самого факта, что утверждение верно

г) верны пункты а) и в)

д) верны пункты а)-в)

7) Примером протокола нулевого разглашения является:

а) гамильтонов цикл для больших графов

б) протокол гроссмейстера

в) RSA

г) варианты а) и б)

д) варианты а)-в)

8) Схема Фейге-Фиата-Шамира базируется на проблеме:

а) дискретного логарифма

б) факторизации

в) преобразования матриц

9) Схема Гиллоу-Куискуотера базируется на проблеме:

а) дискретного логарифма

б) факторизации

в) преобразования матриц

10) Схема Гиллоу-Куискуотера

а) является расширение более раннего протокола Фиата — Шамира

б) является расширением схемы Фейге-Фиата-Шамира

в) не является расширением других протоколов

Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 2

Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ

Модуль *Криптографические методы защиты информации*

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Каннер Татьяна Михайловна,		ведущий инженер лаборатории прикладных исследований	МФТИ-Сбербанк

1. **ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ** *Методология проектирования защищенных информационных систем*

Таблица 2

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
ПК 2. Способен проводить анализ безопасности компьютерных систем.	З-1 Принципы построения компьютерных систем и сетей З-2 Уязвимости компьютерных систем и сетей З-3 Криптографические методы защиты информации З-4 Принципы построения систем управления базами данных З-5 Средства анализа конфигураций З-6 Национальные, межгосударственные и международные стандарты в области защиты информации З-7 Нормативные правовые акты в области защиты информации З-8 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-9 Организационные меры по защите информации У-1

	Анализировать компьютерную систему с целью определения уровня защищенности и доверия У-2 Прогнозировать возможные пути развития действий нарушителя информационной безопасности У-3 Производить анализ политики безопасности на предмет адекватности У-4 Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах У-5 Составлять и оформлять аналитический отчет по результатам проведенного анализа У-6 Разрабатывать предложения по устранению выявленных уязвимостей П-1 Определение уровня защищенности и доверия в компьютерных системах П-2 Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем П-3 Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам П-4 Подготовка аналитического отчета по результатам проведенного анализа П-5 Формулирование предложений по устранению выявленных уязвимостей

5. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

5.1. Распределение объема времени по видам учебной работы

Таблица 2

№ п/п	Наименование дисциплины модуля	Объем времени, отведенный на освоение дисциплины модуля								
		Аудиторные занятия, час.				Промежуточная аттестация (форма итогового контроля /час.)	Контактная работа (час.)	Самостоятельная работа студента, включая текущую аттестацию (час.)	Всего по дисциплине	
		Занятия лекционного типа	Практические занятия	Лабораторные работы	Всего				Час.	Зач. ед.
1	2	3	4	5	6	7	8	9	10	11
2.	Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ	36		18	54	Э	64,35	45,65	108	3
Всего на освоение дисциплины модуля (час.)		18		36	54	З	64,35	45,65	108	3

5.2. Виды СРС, количество и объем времени на контрольно-оценочные мероприятия СРС по дисциплине

Контрольно-оценочные мероприятия СРС включают самостоятельное изучение материала, подготовку к аудиторным занятиям и мероприятиям текущего контроля, выполнение и оформление внеаудиторных мероприятий текущего контроля и подготовку к мероприятиям промежуточного контроля.

Таблица 3

№ п/п	Вид самостоятельной работы студента по дисциплине модуля	Количество контрольно-оценочных мероприятий СРС	Объем контрольно-оценочных мероприятий СРС (час.)
1.	*Подготовка к лекционным*	*6*	*10 час.*
2	*Подготовка к практическим занятиям*	*16*	*16 час.*
3.	*Самостоятельное изучение материала*		*15,65*
	Подготовка к зачету	1	8 час.
	Итого на СРС по дисциплине:		45,65 *час.*

6. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

3.1 В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Личностные качества	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

3.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)

2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

7. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ДИСЦИПЛИНЕ МОДУЛЯ

Зачет в форме итогового тестирования с использованием ОК при реализации модели исключительно электронного обучения с использованием внутреннего онлайн-курса (ОК) УрФУ : http://courses.openedu.urfu.ru/courses/course-v1:UrFU+AOVZ+spring_2018/info

Спецификация теста в системе ОК УрФУ:

Для проведения промежуточной аттестации используется ОК УрФУ.

Структура тестовых материалов при использовании ОК УрФУ: Тест включает в себя 40 заданий, время выполнения – 60 минут. В структуре теста представлены вопросы по всем разделам изучения дисциплины.

Перечень типовых (примерных) тем домашних заданий

1) Установка СЗИ НСД «Аккорд-АМДЗ».
2) Настройка СЗИ НСД «Аккорд-АМДЗ».
3) Установка ПАК СЗИ НСД «Аккорд-Win64».
4) Создание пользователей ПАК СЗИ НСД «Аккорд-Win64» (TSE).
5) Назначение прав доступа пользователей ПАК СЗИ НСД «Аккорд-Win64» (TSE).
6) Установка файлов на контроль целостности в ПАК СЗИ НСД «Аккорд-Win64» (TSE).
7) Задание правил разграничения доступа с использованием дискреционного механизма в ПАК СЗИ НСД «Аккорд-Win64» (TSE).
8) Настройка уровня доступа пользователей и настройка уровня конфиденциальности (меток допуска) объектов в ПАК СЗИ НСД «Аккорд-Win64» (TSE).
9) Изучение работы настроенного комплекса ПАК СЗИ НСД «Аккорд-X».