

**Приложение**  
**к рабочей программе модуля (дисциплины)**

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ**

<b>Код модуля</b>	<b>Модуль</b>
<i>1156040</i>	<i>Гуманитарные аспекты информационной безопасности</i>

**Екатеринбург, 2021**

Оценочные материалы по модулю составлены авторами:

<b>№ п/п</b>	<b>Фамилия Имя Отчество</b>	<b>Ученая степень, ученое звание</b>	<b>Должность</b>	<b>Подразделение</b>
1	Поршнеv Сергей Владимирович	д.т.н., профессор	Директор Учебно-научный центр «Информационн ая безопасность»	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)**  
**Гуманитарные аспекты информационной безопасности**

<b>№ п/п</b>	<b>Перечень дисциплин модуля в последовательности их освоения</b>	<b>Объем дисциплин модуля и всего модуля в зачетных единицах и часах</b>	<b>Форма итоговой промежуточной аттестации по дисциплинам модуля и в целом по модулю</b>
1.	<b>Актуальные проблемы философии и истории науки</b>	<i>3/108</i>	3
2	<b>Основы научного исследования</b>	<i>3/108</i>	3
3	<b>Правовые аспекты информационной безопасности ИСПДн, ГИС и значимых объектов КИИ</b>	<i>3/108</i>	3
4	<b>Профессиональный иностранный язык</b>	<i>3/108</i>	3
ИТОГО по модулю:		<b><i>12/432</i></b>	

**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 *Гуманитарные аспекты информационной безопасности*

Дисциплина *Актуальные проблемы философии и истории науки*

Оценочные материалы составлены автором(ами):

<b>№ п/п</b>	<b>Фамилия Имя Отчество</b>	<b>Ученая степень, ученое звание</b>	<b>Должность</b>	<b>Подразделение</b>
1	Поршнева Ольга Сергеевна	д.и.н., профессор	профессор	<i>Учебно-научный центр «Информационная безопасность»</i>

**4. 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)
<p>УК-4 — Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p>	<p>-1 — современные средства информационно-коммуникационных технологий;                      3-2 — языковой материал (лексические единицы и грамматические структуры), необходимый и достаточный для общения в различных средах и сферах речевой деятельности                      У-1 — воспринимать на слух и понимать содержание аутентичных общественно-политических, публицистических (медийных) и прагматических текстов, относящихся к различным типам речи, выделять в них значимую информацию;                      У-2 — понимать содержание научно-популярных и научных текстов, блогов/веб-сайтов;                      У-3 — выделять значимую информацию из прагматических текстов справочно-информационного и рекламного характера;                      У-4 — вести диалог, соблюдая нормы речевого этикета, используя различные стратегии; выстраивать монолог;                      У-5 — составлять деловые бумаги, в том числе оформлять Curriculum Vitae/Resume и сопроводительное письмо, необходимые при приеме на работу;                      У-6 — вести запись основных мыслей и фактов (из аудиотекстов и текстов для чтения), запись тезисов устного выступления/письменного доклада по изучаемой проблеме;                      У-7 — поддерживать контакты при помощи электронной почты                      П-1 — практическими навыками использования современных коммуникативных технологий;                      П-2 – грамматическими категориями изучаемого (ых) иностранного (ых) языка (ов).</p>

**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
-------	--------------------------------	---

1	2	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.	<i>Актуальные проблемы философии и истории науки</i>	36	-	18	54	Э	62,35	43,57	108	3
<b>Всего на освоение дисциплины модуля (час.)</b>		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-оценочных мероприятий СРС	Объем контрольно-оценочных мероприятий СРС (час.)
1.	<i>Подготовка к лекционным</i>	6	10 час.
2	<i>Подготовка к практическим занятиям</i>	16	16 час.
3.	<i>Самостоятельное изучение материала</i>		8,57
	Подготовка к экзамену	1	9 час.
<b>Итого на СРС по дисциплине:</b>			<b>43,57 час.</b>

## 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).

**Критерии оценивания учебных достижений обучающихся**

<b>Результаты обучения</b>	<b>Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам</b>
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).

**Шкала оценивания достижения результатов обучения (индикаторов) по уровням**

<b>Характеристика уровней достижения результатов обучения (индикаторов)</b>				
<b>№ п/п</b>	<b>Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)</b>	<b>Шкала оценивания</b>		
		<b>Традиционная характеристика уровня</b>		<b>Качественная характеристика уровня</b>
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,	Неудовлетворительно	Не зачтено	Недостаточный (Н)

	имеются существенные ошибки и замечания, требуется доработка	(менее 40 баллов)		
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](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.

##### 3. Примерная тематика самостоятельной работы:

1. Научная революция XVI-XVII вв. и ее влияние на изменение теоретических подходов к познанию.
2. Научное знание в век Просвещения. Становление критического метода исследования
3. Учение Гегеля и его влияние на методологию познания. Законы диалектики.
4. Позитивистская парадигма и развитие методов научных исследований.
5. Марксизм как методология социальных и гуманитарных наук: эвристические возможности и ограничения.
6. Методологическая революция на руб. 19-20 в. и ее влияние на развитие методов познания. Неокантианство. Феноменология. Герменевтика.
7. Неопозитивизм. Методы неопозитивизма и их роль в научных исследованиях.
8. Критический рационализм К. Поппера.
9. Школа модернизации: возникновение, эволюция, влияние на методологию исследований.
10. Теория научных революций Т. Куна.
11. Эпоха постмодернизма и ее влияние на развитие методологии научного познания.
12. Междисциплинарная парадигма современного социогуманитарного знания: причины формирования, методологические и методические аспекты.
13. Теория синергетики: эвристический потенциал, возможности и ограничения.
14. Методология и методы изучения человека и общества в эпоху пост-постмодернизма (нач. XXI века).

##### 4.

Примерный перечень тем домашних работ

1. Критический рационализм К. Поппера.
2. Структурализм как научная парадигма. Влияние структурализма на развитие социальных и гуманитарных наук.
3. Теория научных революций Т. Куна.
4. Эпоха постмодернизма и ее влияние на развитие методологии научного познания.



5. Междисциплинарная парадигма современного социогуманитарного знания: причины формирования, методологические и методические аспекты.
6. Теории систем и их роль в современном познании.
7. Теория синергетики как междисциплинарная парадигма познания.
8. Модели и методы познания в эпоху пост- постмодернизма (нач. XXI века).
9. Количественные методы исследования: место в системе методов, разновидности, условия и сферы применения.
10. Информационные технологии в научных исследованиях.

#### Примерная тематика контрольных работ

1. Общая и специальные теории систем.
2. Теория синергетики: эвристический потенциал, возможности и ограничения. Г. Хакен. И. Пригожин.
3. Институциональный и неинституциональный анализ.
4. Подходы и методы клиометрики и клиодинамики.
5. Герменевтика как методология и метод познания.
6. Моделирование как метод познания.
7. Ментальные карты; интеллект-карты (Mind Maps )
8. Имагология как междисциплинарная научная парадигма. Методы имагологии.

### Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 2

Основы научного исследования

Модуль *Гуманитарные аспекты информационной безопасности*

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	<u>Каннер Татьяна Михайловна,</u>		<u>ведущий инженер лаборатории прикладных исследований</u>	<u>МФТИ-Сбербанк</u>
2	<u>Конявская Светлана Валерьевна,</u>		<u>старший научный сотрудник лаборатории прикладных исследований</u>	<u>МФТИ-Сбербанк</u>

**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)
<p>УК-4 — Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p>	<p>-1 — современные средства информационно-коммуникационных технологий;            3-2 — языковой материал (лексические единицы и грамматические структуры), необходимый и достаточный для общения в различных средах и сферах речевой деятельности            У-1 — воспринимать на слух и понимать содержание аутентичных общественно-политических, публицистических (медийных) и прагматических текстов, относящихся к различным типам речи, выделять в них значимую информацию;            У-2 — понимать содержание научно-популярных и научных текстов, блогов/веб-сайтов;            У-3 — выделять значимую информацию из прагматических текстов справочно-информационного и рекламного характера;            У-4 — вести диалог, соблюдая нормы речевого этикета, используя различные стратегии; выстраивать монолог;            У-5 — составлять деловые бумаги, в том числе оформлять Curriculum Vitae/Resume и сопроводительное письмо, необходимые при приеме на работу;            У-6 — вести запись основных мыслей и фактов (из аудиотекстов и текстов для чтения), запись тезисов устного выступления/письменного доклада по изучаемой проблеме;            У-7 — поддерживать контакты при помощи электронной почты            П-1 — практическими навыками использования современных коммуникативных технологий;            П-2 – грамматическими категориями изучаемого (ых) иностранного (ых) языка (ов).</p>

**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.	Основы научного исследования	36		18	54	Э	64,35	45,65	108	3
<b>Всего на освоение дисциплины модуля (час.)</b>		18		36	54	3	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**

<b>Результаты обучения</b>	<b>Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам</b>
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**

<b>Характеристика уровней достижения результатов обучения (индикаторов)</b>				
<b>№ п/п</b>	<b>Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)</b>	<b>Шкала оценивания</b>		
		<b>Традиционная характеристика уровня</b>		<b>Качественная характеристика уровня</b>
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](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.

#### 1. Компетенции, формируемые в процессе изучения дисциплины

Освоение дисциплины направлено на формирование у обучающегося следующих общекультурных и профессиональных компетенций:

- способность к абстрактному мышлению, анализу, синтезу (ОК-1);
- способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения (ОК-2);
- способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8).

#### 2. Показатели оценивания компетенций

В результате освоения дисциплины обучающийся должен:

##### Знать:

- методологические основы научного познания;
- методы проведения основных этапов научного исследования;
- признаки корректно сформулированной гипотезы;
- порядок оформления и представления результатов научной работы.

##### Уметь:

- планировать эксперимент;
- описывать эксперимент;
- определять границы необходимой и достаточной для конкретного исследования истории вопроса;

- писать аналитические рефераты;
- формулировать гипотезу и проверять корректность ее формулировки;
- оформлять результаты исследования по заданным для того или иного типа работ требованиям;
- использовать MOOK для самостоятельного приобретения знаний, умений и навыков.

**Владеть:**

- научным дискурсом;
- навыками анализа литературы и отбора источников для собственного исследования;
- навыками корректного цитирования и научной полемики;
- навыками самостоятельного приобретения знаний, умений и навыков с использованием MOOK.

**3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю**

В процессе освоения дисциплины предусмотрено выполнение домашних заданий на самопроверку (*без оценивания результатов*). Примерные темы домашних заданий приведены ниже.

**Перечень типовых (примерных) тем домашних заданий**

- 1) Анализ источников, систематизация материала и его визуализация.
- 2) Системность понимания предметной области собственного исследования, отрефлексированное использование обоснований различных видов.
- 3) Анализ определений, используемых в собственном исследовании, в различных аспектах – качества, типа, уместности и пр.
- 4) Рефлексия относительно применения методов научного познания в собственном исследовании – их мотивированность, уместность и достаточность:
  - а) Составление предварительного списка литературы для реферата на заданную тему
  - б) Анализ двух выбранных статей, одна из которых оценивается учащимся как хорошая, а вторая – как плохая.
  - в) Доработка по пройденным рекомендациям собственной новой или ранее написанной статьи.

В онлайн-курсе, с помощью которого реализуется дисциплина предусмотрено 2 (две) проверочные работы (в виде теста, размещенного на онлайн-платформе MOOK). Примерный вариант тестов по каждому разделу приведен ниже.

**Перечень типовых (примерных) вопросов для проведения текущего контроля знаний**

(\*) – помечены правильные ответы

1. Проверочная работа по темам «Введение», «Обоснования и доказательства», «Определения», «Ошибки»

1) Какие признаки научности скрываются за метафорой «научной честности» в эссе Фейнмана «Наука самолетопоклонников»?

Можно отметить любое количество ответов. В ветке форума можно привести аргументы для каждого отмеченного признака – цитату или пересказ того фрагмента эссе, где идет речь об этой характеристике.

- (\*) цель – установление истины
- (\*) задача – описание мира, выявление объективных законов
- (\*) реализм
- проблемность (полезность)
- обоснованность
- (\*) эмпиричность
- (\*) объективность
- (\*) системность
- (\*) теоретичность
- (\*) воспроизводимость
- (\*) верифицируемость
- дискурсивность
- применение специального инструментария
- определенность и постоянство понятий
- (\*) определенность и постоянство методологии исследовательских процедур
- (\*) совместимость
- (\*) прогрессивное развитие
- (\*) опровержимость
- принципы (простоты, консерватизма, универсальности, красоты)

*(примечание для проверяющего: если пропущен один из отмеченных ответов, то ответ неверный, если отмечено больше ответов, то ответ засчитывается как правильный, если лишние ответы разумно мотивированы в ветке форума – учесть в каких-нибудь поощрительных баллах).*

2) Может ли исследование соответствовать признаку «совместимость», если в нем опровергаются ранее полученные результаты и ранее построенные теории?

– нет, не может, так как «совместимость» – это основанность на прежних результатах и теориях, если они опровергнуты, то исследование не «совместимо»;

– нет, не может, так как «совместимость» и «прогрессивность» находятся в дополнительной дистрибуции – если есть одно, не может быть другого, если исследование «прогрессивно», оно не «совместимо»;

– (\*) да, может, так как «совместимость» – это возможность соотнесения нового исследования с прежними, включая их опровержение, если такая возможность есть, исследование «совместимо»;

– да, может, так как для «совместимости» достаточно, чтобы исследования касались одного и того же предмета изучения, если исследуется тот же предмет, исследование «совместимо».

3) Знание какого типа можно обосновать путем дедуктивного рассуждения?

- никакого;
- (\*) описание (констатация);
- объяснение (выявление причины);
- предсказание;



- любого типа.
- 4) Если нам известно сложное следствие сложной причины, и известна причина части этого сложного следствия, то, вероятно, оставшаяся часть следствия вызвана оставшейся частью причины. Что это?
- индукция, принцип единственного сходства
  - дедукция, закон исключенного третьего
  - индукция, закон непротиворечия
  - индукция, закон тождества
  - дедукция, принцип единственного различия
  - дедукция, принцип сопутствующих изменений
  - (\*) индукция, принцип остатков
  - закон достаточности оснований
  - дедукция, закон непротиворечия
  - дедукция, закон тождества
  - индукция, принцип единственного различия
  - индукция, принцип сопутствующих изменений
  - дедукция, принцип остатков
- 5) Что из перечисленного не зависит от среды в теории образов Гренандера?
- (\*) образ (image)
  - изображение (pattern)
  - (\*) абстрактная образующая
  - конкретная образующая
- 6) Чье это определение? «Информация есть сущность, сохраняющаяся при вычислимом изоморфизме»
- народное
  - Н. Виннера
  - (\*) А. Н. Колмогорова
  - В. А. Конявского
  - Л. А. Заде
  - М. Л. Мински
- 7) Определение составлено без ошибок, если
- оно реальное;
  - оно номинальное;
  - (\*) оно соответствует действительности, если реальное, и оно целесообразно, если номинальное;
  - оно соответствует действительности;
  - оно продуктивно;
  - оно целесообразно;
  - оно целесообразно, продуктивно и соответствует действительности;
  - оно продуктивно, если реальное, и оно целесообразно, если номинальное.
- 8) Классические научные определения – это
- номинальные определения, построенные на основании связи «тождество»;
  - любые номинальные определения;
  - любые реальные определения;
  - реальные определения, построенные на основании связи «часть/целое»;
  - (\*) реальное определение, построенное на основании связи «род/вид»;

- продуктивное и соответствующее действительности реальное определение;
- целесообразное и продуктивное номинальное определение;
- продуктивное определение (целесообразное, если номинальное, и соответствующее действительности, если реальное).

9) Какой ошибки не сделано в выводе о том, что таракан слышит ногами? Отметьте сколько угодно вариантов, поясните их в ветке форума...

- (\*) языковой
- (\*) арифметической
- методологической
- методической
- фактической
- (\*) терминологической
- ошибки чувственного восприятия
- логической
- системной
- (\*) хронологической
- в этом выводе нет ошибки
- свой ответ

*(примечание для проверяющего: если учащийся отметит, что есть терминологическая или языковая ошибка – можно не засчитывать за ошибку, так как слово «слышать» в русском языке просторечно используется в значение «ощущать», «осознать» и даже «обонять», и в этом смысле можно считать такую ошибку за терминологическую или языковую, но только если эта позиция отражена в пояснении в ветке форума, так как в английском языке такие особенности отсутствуют, и эта логика не самоочевидна).*

10) Какие ошибки в исследовании обязательно следует исправлять, даже если исследование уже введено в научный оборот? В ответе укажите буквенные обозначения вариантов в алфавитном порядке без пробелов (например, «abcdeg»)

- a. любые
- b. те, что явно бросаются в глаза
- c. те, что легко исправить
- d. системные
- e. те, что влияют на логику доказательства
- f. те, что не меняют логику доказательства
- g. фактические
- h. ошибки чувственного восприятия
- i. те, что касаются положений, следствия которых используются в дальнейшем рассуждении

j. никакие: что введено в научный оборот, то введено

(\*) Правильные ответы:

ei, bei, cei, dei, efi, egi, ehi, bcei, bdei, befi, begi, behi, cdei, cefi, cegi, cehi, defi, degi, dehi, efgi, efhi, eghi, bcdei, bcefi, bcegi, bcehi, bdefi, bdegi, bdehi, befgi, befhi, beghi, cdefi, cdegi, cdehi, cefgi, cefhi, ceghi, defgi, defhi, deghi, efgi, bcdefi, bcdegi, bcdehi, bcefgi, bcefhi, bceghi, bdefgi, bdefhi, bdeghi, befghi, cdefgi, cdefhi, cdeghi, cefghi, defghi, bcdefgi, bcdefhi, bcdeghi, bcefghi, bdefghi, cdefghi, bcdefghi.

2. Проверочная работа по темам «Понятия метод, методика, методология, направление», «Работа исследователя и исследовательская работа», «История вопроса», «Экспериментальная», «Научный дискурс», «Защита диссертации – не самооборона»

1) Какие методы научного познания обнаруживаются в составе метода «восхождение от абстрактного к конкретному»?

Ответ может состоять из нескольких пунктов. Он должен представлять собой перечень номеров ответов по алфавиту без пробелов и знаков препинания, в нижнем регистре (например, abcdefghij)

- a. абстрагирование
- b. анализ
- c. синтез
- d. индукция
- e. дедукция
- f. моделирование
- g. исторический метод
- h. идеализация
- i. формализация
- j. аксиоматический метод

(\*) Правильный ответ: abcfhi

2) Методом чего является взвешивание?

- доказательства
- научного познания
- моделирования
- (\*) измерения
- ничего из перечисленного
- всего перечисленного

3) Результат реферата должен

- давать работоспособное техническое решение
- быть новым и актуальным
- быть связан с научной проблемой
- (\*) быть ответом на вопрос
- раскрывать тему реферата
- быть экспериментально проверен

4) Цель диссертации или диплома\* актуальна, если

- ее прежде не ставили
- ее прежде не достигли
- (\*) она связана с нерешенной научной проблемой
- она связана с практической задачей, на которую есть спрос
- ее утвердили на кафедре

Примечание: в рамках этого курса считаем, что диплом – это научное исследование, дипломы, представляющие собой технический проект, не учитываются, так как не относятся к предметной области курса «Основы научного исследования»

5) «Разработка способа проверки эффективности обеспечения X путем Y» - что будет корректной формой результата для диплома на такую тему?

- доказательство, что обеспечение X путем Y – эффективно
- описание способа обеспечения X путем Y
- (\*) описание способа проверки эффективности обеспечения X путем Y
- исследование основных параметров, влияющих на эффективность обеспечения

X путем Y

- методика проверки эффективности обеспечения X путем Y
- любой из этих результатов

6) Как соотносятся предмет и объект исследования?

- объект шире, чем предмет
- объект уже, чем предмет
- объект – это конкретное, а предмет – абстрактное
- (\*) предмет – это то, что именно исследуется в объекте
- объект – это то, что именно исследуется в предмете
- предмет – это область знания, а объект – это то, что исследуется
- предмет шире, чем объект
- предмет – это конкретное, а объект – абстрактное
- это одно и то же
- они не соотносятся

7) Почему практическая часть научного исследования называется экспериментальной?

- это традиция
- потому что никогда не знаешь точно, что получится
- (\*) потому что задача этой части – проверка гипотезы практикой
- потому что результат этой части – новое, экспериментальное решение

8) Использование методов математической статистики в экспериментальной части

– обязательно, так как планирование эксперимента – это раздел математической статистики

– не требуется, так как экспериментальная часть – практическая, а математическая статистика – это вычисление

- (\*) должно быть обосновано, как применение любых методов
- желательно, так как снижение дисперсии и рандомизация эксперимента

существенно повышают точность результата

9) Почему за вопросы и замечания на защите нужно благодарить?

- это традиция
- это вежливо
- потому что заслуженные люди удостоили вниманием вашу работу
- потому что они помогают посмотреть на свою работу по-новому и открывают

перспективы

- (\*) по всем перечисленным причинам

10) Что из нижеперечисленного не будет нарушением научного дискурса

- запрет на вопросы докладчику
- отказ докладчика отвечать на вопросы
- (\*) использование аналогий при объяснении своей позиции
- работа, написанная в стихах

- дипломная работа, распечатанная на бумаге формата А5
- использование шрифта В52 или **ALGERIAN**
- все перечисленное является нарушением научного дискурса

### **Критерии и шкалы оценивания**

Оценивание результатов каждой текущего контроля знаний осуществляется в соответствии со следующими критериями и шкалами:

Шкала оценивания	Критерий оценивания
«отлично» (80-100 баллов)	Обучающийся верно ответил на 80% и более вопросов теста текущего контроля знаний. Обучающийся показал полное освоение планируемых результатов (знаний, умений, навыков, компетенций), предусмотренных темами дисциплины
«хорошо» (60-79 баллов)	Обучающийся верно ответил на 60-79% вопросов теста текущего контроля знаний. Обучающийся показал освоение планируемых результатов (знаний, умений, навыков, компетенций), предусмотренных темами дисциплины, но допустил некоторые неточности при прохождении текущего контроля знаний
«удовлетворительно» (40-59 баллов)	Обучающийся верно ответил на 40-59% вопросов теста текущего контроля знаний. Обучающийся показал освоение планируемых результатов (знаний, умений, навыков, компетенций), предусмотренных темами дисциплины, со значительными погрешностями при прохождении текущего контроля знаний
«неудовлетворительно» (менее 40 баллов)	Обучающийся верно ответил менее, чем на 40% вопросов теста текущего контроля знаний. Обучающийся не показал освоение планируемых результатов (знаний, умений, навыков, компетенций), раздела дисциплины

### Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 3

*Правовые аспекты информационной безопасности ИСПДн, ГИС и значимых объектов  
КИИ*

*Модуль Гуманитарные аспекты информационной безопасности*

<b>№ п/п</b>	<b>Фамилия Имя Отчество</b>	<b>Ученая степень, ученое звание</b>	<b>Должность</b>	<b>Подразделение</b>
1	Каннер Татьяна Михайловна,		ведущий инженер лаборатории прикладных исследований	МФТИ-Сбербанк
2	Чадов Антон Юрьевич,		старший преподаватель	кафедры защиты информации МИФИ

**2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ *Правовые аспекты информационной безопасности ИСПДн, ГИС и значимых объектов КИИ***

Таблица 2

Код и наименование компетенций, формируемые с участием дисциплины	Планируемые результаты обучения (индикаторы)
<p>УК-4 — Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p>	<p>-1 — современные средства информационно-коммуникационных технологий;            З-2 — языковой материал (лексические единицы и грамматические структуры), необходимый и достаточный для общения в различных средах и сферах речевой деятельности            У-1 — воспринимать на слух и понимать содержание аутентичных общественно-политических, публицистических (медийных) и прагматических текстов, относящихся к различным типам речи, выделять в них значимую информацию;            У-2 — понимать содержание научно-популярных и научных текстов, блогов/веб-сайтов;            У-3 — выделять значимую информацию из прагматических текстов справочно-информационного и рекламного характера;            У-4 — вести диалог, соблюдая нормы речевого этикета, используя различные стратегии; выстраивать монолог;            У-5 — составлять деловые бумаги, в том числе оформлять Curriculum Vitae/Resume и сопроводительное письмо, необходимые при приеме на работу;            У-6 — вести запись основных мыслей и фактов (из аудиотекстов и текстов для чтения), запись тезисов устного выступления/письменного доклада по изучаемой проблеме;            У-7 — поддерживать контакты при помощи электронной почты            П-1 — практическими навыками использования современных коммуникативных технологий;            П-2 – грамматическими категориями изучаемого (ых) иностранного (ых) языка (ов).</p>

## 8. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

### 8.1. 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
3.	Правовые аспекты информационной безопасности ИСПДн, ГИС и значимых объектов КИИ	36		18	54	Э	64,35	45,65	108	3
<b>Всего на освоение дисциплины модуля (час.)</b>		18		36	54	3	64,35	45,65	108	3

### 8.2. 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.
-----------------------------	------------

## 9. 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

## 10. 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](http://courses.openedu.urfu.ru/courses/course-v1:UrFU+AOVZ+spring_2018/info)

Спецификация теста в системе ОК УрФУ:

### 1. Перечень типовых (примерных) вопросов текущего контроля знаний

1. Контрольная работа по теме «Правовые основы обеспечения информационной безопасности»

1) Юридическое определение информации:

а) сведения (сообщения, данные), независимо от формы их представления;

б) сведения, зафиксированные на материальном носителе;

в) сообщения и (или) данные, ставшие общедоступными.

г) любые сообщения и данные, доступные для восприятия человеком.

2) Категории информации по условиям доступности/недоступности:

а) общедоступная информация и информация ограниченного доступа;

б) общедоступная информация и конфиденциальная информация;

в) информация, доступ к которой не может быть ограничен, и закрытая информация.

г) сведения, составляющие государственную тайну, и сведения конфиденциального характера.

3) Ограничение доступа к информации возможно в целях:

а) защиты основ конституционного строя;

б) нравственности, здоровья, прав и законных интересов других лиц;

в) обеспечения обороны страны и безопасности государств;

г) всё вышеперечисленное.

4) Конфиденциальность информации это:

а) обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

б) принцип неразглашения информации, не предназначенной для открытого доступа;

в) свойство информации быть известной только доверенным лицам.

5) Основные нормативные правовые акты в области информационной безопасности:

а) федеральный закон «Об информационной безопасности»;

б) Доктрина информационной безопасности Российской Федерации;

в) национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности»;

г) все варианты;

д) варианты «б» и «в».

б) Обладатель информации это:

а) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

б) физическое лицо, самостоятельно создавшее информацию и зафиксировавшее её на материальном носителе;

в) юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

7) Юридически значимые признаки информации, составляющей коммерческую тайну, определены в:

а) федеральном законе «О коммерческой тайне»;

б) федеральном законе «О коммерческой деятельности»;

в) федеральном законе «Об информационной безопасности».

8) К профессиональным тайнам относятся:

а) коммерческая тайна;

б) банковская тайна;

в) врачебная тайна, адвокатская тайна, тайна нотариальных действий, тайна связи.

г) все вышеперечисленные.

9) Трансрежимность сведений конфиденциального характера это:

а) возможность защиты сведений в один и тот же отрезок времени без изменения их содержания с позиций разных правовых режимов;

б) возможность передачи сведений конфиденциального характера третьим лицам без согласия их первоначального обладателя;

в) невозможность отнесения сведений конфиденциального характера к государственной тайне.

10) Ключевыми стандартами в области обеспечения безопасности информации являются:

а) стандарты ИСО/МЭК серии 27000;

б) стандарты ИСО/МЭК серии 17700;

в) стандарты ИСО/МЭК серии 12207.

## 2. Контрольная работа по теме «Правовые аспекты ИБ персональных данных»

1) Персональные данные, это:

а) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

б) сведения о физическом лице, ставшие общедоступными;

в) сведения о человеке, накопленные в ИСПДн.

2) К специальным категориям персональных данных относятся:

а) сведения о расовой, национальной принадлежности;

б) сведения о политических взглядах, религиозных или философских убеждениях;

в) сведения о состоянии здоровья, интимной жизни;

г) все вышеперечисленные.

3) Обезличивание персональных данных это:

а) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

б) действия, в результате которых из персональных данных удалены изображения субъекта персональных данных;

в) действия, в результате которых персональные данные невозможно извлечь из информационной системы персональных данных.

4) Государственная дактилоскопическая регистрации обязательна для:

а) физических лиц, указанных в ст. 9 Федерального закона от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации».

б) физических лиц, занимающихся экстремальными видами спорта;

в) физических лиц, страдающих редкими и опасными заболеваниями.

5) Согласие субъекта на обработку его персональных данных делается:

а) в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом;

б) только в письменной форме;

в) согласия не требуется.

6) Уполномоченным органом по защите прав субъектов персональных данных является:

а) Роскомнадзор;

б) ФСБ России;

в) ФСТЭК России.

7) Требования к защите персональных данных при их обработке в информационных системах персональных данных утверждены:

а) постановлением Правительства РФ от 01.11.2012 № 1119;

б) постановлением Правительства РФ от 13.06.2012 № 584;

в) постановлением Правительства РФ от 15.09.2008 № 687.

8) Установленные уровни защищённости персональных данных при их обработке в информационных системах персональных данных:

а) 4 уровня защищённости;

б) 3 уровня защищённости;

в) 5 уровней защищённости.

9) Организационные и технические меры обеспечения безопасности персональных данных определены в:

- а) приказе ФСТЭК России от 18.02.2013 № 21.
- б) приказе Роскомнадзора от 30.05.2017 № 94.
- в) Федеральном законе от 27.06.2006 № 152-ФЗ «О персональных данных».
- г) Доктрине информационной безопасности Российской Федерации.

10) За нарушение законодательства о персональных данных установлена следующая юридическая ответственность:

- а) все виды юридической ответственности.
- б) административная.
- в) административная и уголовная.
- г) дисциплинарная и гражданско-правовая.

3. Контрольная работа по теме «Правовые аспекты ИБ государственных информационных систем»

1) Под информационной системой понимается:

- а) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- б) технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- в) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

2) Государственные информационные системы создаются на основе:

- а) статистической информации, предоставляемой физическими лицами, организациями, государственными органами, органами местного самоуправления;
- б) иной документированной информации, предоставляемой физическими лицами, организациями, государственными органами, органами местного самоуправления;
- в) любой информации, предоставляемой государственными органами и органами местного самоуправления;
- г) варианты «а» и «б».

3) Единая система идентификации и аутентификации это:

- а) федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах;

б) информационная система, которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах;

в) государственная информационная система, которая ограничивает в случаях, предусмотренных законодательством Российской Федерации, доступ к информации, содержащейся в информационных системах.

4. Требования о защите информации, не составляющей государственную тайну, содержащейся в ГИС установлены:

- а) приказом ФСТЭК России от 11.02.2013 № 17;
- б) постановлением Правительства Российской Федерации от 06.07.2015 № 676.

- в) Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
- г) внутренними распорядительными документами собственника ГИС.
- 5) Банк данных угроз безопасности информации создаёт и ведёт:
  - а) ФСТЭК России;
  - б) ФСБ России;
  - в) Роскомнадзор;
  - г) Все вышеперечисленные органы.
- б) Требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации утверждены:
  - а) ФСБ России.
  - б) ФСТЭК России.
  - в) Минкомсвязи России;
  - г) Правительством Российской Федерации.
- 7) Применение электронной подписи регулируется:
  - а) Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
  - б) Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»;
  - в) Федеральным законом от 07.07.2003 № 126-ФЗ «О связи».
- 8) Видами электронных подписей в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» являются:
  - а) простая электронная подпись;
  - б) непростая электронная подпись;
  - в) простая неквалифицированная электронная подпись;
  - г) усиленная неквалифицированная электронная подпись;
  - д) усиленная квалифицированная электронная подпись.
  - е) все варианты.
  - ж) варианты «а», «г» и «д».
- 9) Лицензирование деятельности в области СКЗИ регулируется:
  - а) Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
  - б) Законом Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне»;
  - в) Постановлением Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении положения «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием Шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, Если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

г) всеми вышеперечисленными нормативными правовыми актами;

д) варианты «а» и «в».

10) Подтверждение соответствия СКЗИ техническим требованиям осуществляется в форме:

а) обязательной сертификации.

б) добровольной сертификации.

в) добровольного декларирования соответствия.

г) обязательного декларирования соответствия.

4. Контрольная работа по теме «Правовые аспекты ИБ значимых объектов критической информационной инфраструктуры»

1) Основным законом о критической информационной инфраструктуре Российской Федерации является:

а) Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

б) Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»;

в) Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о безопасности информации».

2) Субъектами критической информационной инфраструктуры не являются:

а) физические лица;

б) государственные органы и государственные учреждения;

в) российские юридические лица и (или) индивидуальные предприниматели.

3) ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» определяет компьютерную атаку как:

а) целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

б) атака, инициированная с компьютера на другой компьютер или веб-сайт с целью нарушения целостности, конфиденциальности или доступности информации;

в) любое неправомерное воздействие на программные и (или) программно-аппаратные средства и информацию.

4) Федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры является:

а) ФСТЭК России;

б) ФСБ России;

в) Роскомнадзор.

5) Категорирование объектов критической информационной инфраструктуры осуществляется в порядке, установленном:

а) постановлением Правительства Российской Федерации от 08.02.2018 № 127;

б) приказами ФСБ России;

в) Федеральным законом от 07.07.2003 № 126-ФЗ «О связи»;

г) внутренними распорядительными документами субъекта КИИ.

б) Установленное количество категорий значимости объектов критической информационной инфраструктуры:

- а) 3 категории значимости;
  - б) 4 категории значимости;
  - в) 6 категорий значимости.
- 7) Реестр значимых объектов критической информационной инфраструктуры ведёт:
- а) ФСТЭК России;
  - б) ФСБ России;
  - в) НКЦКИ;
  - г) Минкомсвязи России.
- 8) Уполномоченным федеральным органом исполнительной власти в сфере ГосСОПКА является:
- а) ФСБ России.
  - б) ФСТЭК России.
  - в) Минкомсвязь России.
- 9) Оценку безопасности значимых объектов критической информационной инфраструктуры осуществляет:
- а) ФСБ России;
  - б) ФСТЭК России;
  - в) Роскомнадзор;
  - г) варианты «а» и «б».
- 10) За неправомерное воздействие на критическую информационную инфраструктуру установлена:
- а) Уголовная ответственность;
  - б) административная ответственность;
  - в) все виды юридической ответственности.

#### **Критерии и шкалы оценивания**

Критерии и шкалы оценивания результатов обучения при проведении текущей аттестации представлены в «Методических рекомендациях по критериям и шкалам оценивания в рамках БРС» УрФУ.

#### **2. 4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся по итогам обучения**

По дисциплине предусмотрена промежуточная аттестация в форме зачета. На зачете студенту предлагается тест из 10 (десяти) заданий с последующим ответом в устной форме. Примерный вариант теста:

- 1) Юридическое определение информации дано в:
  - а) Федеральном законе от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о безопасности информации»;
  - б) Федеральном законе от 07.07.2003 № 126-ФЗ «О связи»;
  - в) Доктрине информационной безопасности Российской Федерации.
- 2) Трансрежимность конфиденциальной информации это:
  - а) возможность защиты одних и тех же сведений без изменения их содержания с позиций разных правовых режимов в один и тот же отрезок времени;
  - б) возможность передачи сведений конфиденциального характера иному обладателю.
  - в) возможность свободного оборота сведений конфиденциального характера.



3) В соответствии с ГОСТ Р ИСО/МЭК 27001-2006 под информационной безопасностью понимается:

а) свойство информации сохранять конфиденциальность, целостность и доступность;

б) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;

в) установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

4) Базовым законом в области персональных данных является:

а) Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»;

б) Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о безопасности информации»;

в) Кодекс Российской Федерации об административных правонарушениях.

г) В

все вышеперечисленные.

5) Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных» установлены следующие категории ПДн:

а) общедоступные ПДн;

б) специальные категории ПДн;

в) биометрические ПДн;

г) обезличенные ПДн;

д) все вышеперечисленные;

е) варианты «а», «б» и «г».

6) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 устанавливает:

а) требования к защите персональных данных при их обработке в информационных системах персональных данных;

б) уровни защищённости персональных данных при их обработке в информационных системах персональных данных;

в) перечень средств защиты информации для системы защиты персональных данных;

г) варианты «а» и «б»;

д) всё вышеперечисленное.

7) Требования о защите информации, не составляющей государственную тайну, содержащейся в ГИС установлены:

а) приказом ФСТЭК России от 11.02.2013 № 17;

б) постановлением Правительства Российской Федерации от 06.07.2015 № 676.

в) Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

8) Требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации утверждены:

а) ФСБ России;

б) ФСТЭК России;

в) Минкомсвязи России;

г) Правительством Российской Федерации.

9) Значимый объект КИИ РФ это:

а) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

б) объект критической информационной инфраструктуры, который включен в реестр значимых объектов критической информационной инфраструктуры;

в) объект критической информационной инфраструктуры, собственником которого является государственный орган.

10) Определение категорий значимости объектов критической информационной инфраструктуры осуществляется на основании:

а) показателей критериев значимости объектов критической информационной инфраструктуры и их значений, утверждённых Правительством Российской Федерации;

б) мотивированного решения федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

в) согласия федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

г) внутренних распорядительных документов субъекта КИИ.

11) Федеральным органом исполнительной власти, наделённым полномочиями в области ГосСОПКА, является:

а) ФСБ России;

б) ФСТЭК России;

в) Минкомсвязи России;

г) МВД России.

### Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 2

Основы научного исследования

Модуль *Гуманитарные аспекты информационной безопасности*

<b>№ п/п</b>	<b>Фамилия Имя Отчество</b>	<b>Ученая степень, ученое звание</b>	<b>Должность</b>	<b>Подразделение</b>
1	Ковалева Александра Георгиевна	Кандидат педагогических наук, доцент	доцент	Кафедра иностранных языков и перевода
2	Чернова Ольга Вячеславовна		Старший преподаватель	Кафедра иностранных языков и образовательных технологий

**3. 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)
<p>УК-4 — Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p>	<p>-1 — современные средства информационно-коммуникационных технологий;            3-2 — языковой материал (лексические единицы и грамматические структуры), необходимый и достаточный для общения в различных средах и сферах речевой деятельности            У-1 — воспринимать на слух и понимать содержание аутентичных общественно-политических, публицистических (медийных) и прагматических текстов, относящихся к различным типам речи, выделять в них значимую информацию;            У-2 — понимать содержание научно-популярных и научных текстов, блогов/веб-сайтов;            У-3 — выделять значимую информацию из прагматических текстов справочно-информационного и рекламного характера;            У-4 — вести диалог, соблюдая нормы речевого этикета, используя различные стратегии; выстраивать монолог;            У-5 — составлять деловые бумаги, в том числе оформлять Curriculum Vitae/Resume и сопроводительное письмо, необходимые при приеме на работу;            У-6 — вести запись основных мыслей и фактов (из аудиотекстов и текстов для чтения), запись тезисов устного выступления/письменного доклада по изучаемой проблеме;            У-7 — поддерживать контакты при помощи электронной почты            П-1 — практическими навыками использования современных коммуникативных технологий;            П-2 – грамматическими категориями изучаемого (ых) иностранного (ых) языка (ов).</p>

**11. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ**

### 11.1. Распределение объема времени по видам учебной работы

Таблица 2

№ п/п	Наименование дисциплины модуля	Объем времени, отведенный на освоение дисциплины модуля								
		Аудиторные занятия, час.				Промежу- точная аттестация (форма итогового контроля /час.)	Конта- ктная работа (час.)	Самостоя- тельная работа студента, включая текущую аттестаци- ю (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
4.	Основы научного исследования	36		18	54	Э	64,35	45,65	108	3
<b>Всего на освоение дисциплины модуля (час.)</b>		18		36	54	3	64,35	45,65	108	3

### 11.2. 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.	<i>Подготовка к лекционным</i>	6	10 час.
2	<i>Подготовка к практическим занятиям</i>	16	16 час.
3.	<i>Самостоятельное изучение материала</i>		15,65
	Подготовка к зачету	1	8 час.
Итого на СРС по дисциплине:			45,65 час.

## 12. 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**

<b>Результаты обучения</b>	<b>Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам</b>
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**

<b>Характеристика уровней достижения результатов обучения (индикаторов)</b>				
<b>№ п/п</b>	<b>Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)</b>	<b>Шкала оценивания</b>		
		<b>Традиционная характеристика уровня</b>		<b>Качественная характеристика уровня</b>
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	Удовлетворительн о (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворител ьно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

### 13. 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](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.

#### Примерные задания для проведения мини-контрольных в рамках учебных занятий

*Choose a correct word to fill the gap.*

#### Information security definition

Information security, sometimes abbreviated to infosec, is a set of practices intended to keep data secure from 1 ... (unauthorized/ authorized) access or alterations, both when it's being stored and when it's being transmitted from one machine or physical location to another. You might sometimes see it referred to as data security. As knowledge has become one of the 21st century's most important assets, efforts to keep information 2 ... (secure/insecure) have correspondingly become increasingly important.

Information security refers to the processes and methodologies which are designed and implemented 3 ... (to protect/to destroy) print, electronic, or any other form of confidential, private and sensitive information or data from 4 ... (unauthorized/authorized) access, use, misuse, disclosure, destruction, modification, or disruption.

#### Перечень примерных вопросов для экзамена/ зачета

*Read the article. Make translation of the highlighted part. Make review of the article.*

#### Information security: all you should know

By Josh Fruhlinger

CSO | JAN 17, 2020 3:00 AM PST

## Information security vs. cybersecurity

Because information technology has become the accepted corporate buzzphrase that means, basically, "computers and related stuff," you will sometimes see information security and cybersecurity used interchangeably. Strictly speaking, cybersecurity is the broader practice of defending IT assets from attack, and information security is a specific discipline under the cybersecurity umbrella. Network security and application security are sister practices to infosec, focusing on networks and app code, respectively.

Obviously, there's some overlap here. You can't secure data transmitted across an insecure network or manipulated by a leaky application. As well, there is plenty of information that isn't stored electronically that also needs to be protected. Thus, the infosec pro's remit is necessarily broad.

## Information security principles

The basic components of information security are most often summed up by the so-called CIA triad: confidentiality, integrity, and availability.

Confidentiality is perhaps the element of the triad that most immediately comes to mind when you think of information security. Data is confidential when only those people who are authorized to access it can do so; to ensure confidentiality, you need to be able to identify who is trying to access data and block attempts by those without authorization. Passwords, encryption, authentication, and defense against penetration attacks are all techniques designed to ensure confidentiality.

Integrity means maintaining data in its correct state and preventing it from being improperly modified, either by accident or maliciously. Many of the techniques that ensure confidentiality will also protect data integrity—after all, a hacker can't change data they can't access—but there are other tools that help provide a defense of integrity in depth: checksums can help you verify data integrity, for instance, and version control software and frequent backups can help you restore data to a correct state if need be. Integrity also covers the concept of non-repudiation: you must be able to prove that you've maintained the integrity of your data, especially in legal contexts.

Availability is the mirror image of confidentiality: while you need to make sure that your data can't be accessed by unauthorized users, you also need to ensure that it can be accessed by those who have the proper permissions. Ensuring data availability means matching network and computing resources to the volume of data access you expect and implementing a good backup policy for disaster recovery purposes.

In an ideal world, your data should always be kept confidential, in its correct state, and available; in practice, of course, you often need to make choices about which information security principles to emphasize, and that requires assessing your data. If you're storing sensitive medical information, for instance, you'll focus on confidentiality, whereas a financial institution might emphasize data integrity to ensure that nobody's bank account is credited or debited incorrectly.

## Information security policy

The means by which these principles are applied to an organization take the form of a security policy. This isn't a piece of security hardware or software; rather, it's a document that an enterprise draws up, based on its own specific needs and quirks, to establish what data needs to be protected and in what ways. These policies guide the organization's decisions around procuring cybersecurity tools, and also mandate employee behavior and responsibilities.



Among other things, your company's information security policy should include:

A statement describing the purpose of the infosec program and your overall objectives

Definitions of key terms used in the document to ensure shared understanding

An access control policy, determining who has access to what data and how they can establish their rights

#### A password policy

A data support and operations plan to ensure that data is always available to those who need it

Employee roles and responsibilities when it comes to safeguarding data, including who is ultimately responsible for information security

One important thing to keep in mind is that, in a world where many companies outsource some computer services or store data in the cloud, your security policy needs to cover more than just the assets you own. You need to know how you'll deal with everything from personally identifying information stored on AWS instances to third-party contractors who need to be able to authenticate to access sensitive corporate info.

#### Information security measures

As should be clear by now, just about all the technical measures associated with cybersecurity touch on information security to a certain degree, but there it is worthwhile to think about infosec measures in a big-picture way:

- Technical measures include the hardware and software that protects data — everything from encryption to firewalls
- Organizational measures include the creation of an internal unit dedicated to information security, along with making infosec part of the duties of some staff in every department
- Human measures include providing awareness training for users on proper infosec practices
- Physical measures include controlling access to the office locations and, especially, data centers

#### Information security jobs

It's no secret that cybersecurity jobs are in high demand, and in 2019 information security was at the top of every CIO's hiring wishlist, according to Mondo's IT Security Guide. There are two major motivations: There have been many high-profile security breaches that have resulted in damage to corporate finances and reputation, and most companies are continuing to stockpile customer data and give more and more departments access to it, increasing their potential attack surface and making it more and more likely they'll be the next victim.

There are a variety of different job titles in the infosec world. The same job title can mean different things in different companies, and you should also keep in mind our caveat from up top: a lot of people use "information" just to mean "computer-y stuff," so some of these roles aren't restricted to just information security in the strict sense. But there are general conclusions one can draw.

#### Information security analyst: Duties and salary

Let's take a look at one such job: information security analyst, which is generally towards the entry level of an infosec career path. CSO's Christina Wood describes the job as follows:

Security analysts typically deal with information protection (data loss protection [DLP] and data classification) and threat protection, which includes security information and event management (SIEM), user and entity behavior analytics [UEBA], intrusion detection system/intrusion prevention system (IDS/IPS), and penetration testing. Key duties include managing security measures and controls, monitoring security access, doing internal and external security audits, analyzing security breaches, recommending tools and processes, installing software, teaching security awareness, and coordinating security with outside vendors.

Information security analysts are definitely one of those infosec roles where there aren't enough candidates to meet the demand for them: in 2017 and 2018, there were more than 100,000 information security analyst jobs that were unfilled in the United States. This means that InfoSec analyst is a lucrative gig: the Bureau of Labor Statistics pegged the median salary at \$95,510 (PayScale.com has it a bit lower, at \$71,398).

### Information security training and courses

How does one get a job in information security? An undergraduate degree in computer science certainly doesn't hurt, although it's by no means the only way in; tech remains an industry where, for instance, participation in open source projects or hacking collectives can serve as a valuable calling card.

Still, infosec is becoming increasingly professionalized, which means that institutions are offering more by way of formal credentials. Many universities now offer graduate degrees focusing on information security. These programs may be best suited for those already in the field looking to expand their knowledge and prove that they have what it takes to climb the ladder.

At the other end of the spectrum are free and low-cost online courses in infosec, many of them fairly narrowly focused. The world of online education is something of a wild west; Tripwire breaks down eleven highly regarded providers offering information security courses that may be worth your time and effort.

### Information security certifications

If you're already in the field and are looking to stay up-to-date on the latest developments—both for your own sake and as a signal to potential employers—you might want to look into an information security certification. Among the top certifications for information security analysts are:

Systems Security Certified Practitioner (SSCP)

Certified Cyber Professional (CCP)

Certified Information System Security Professional (CISSP)

Certified Ethical Hacker (CEH)

GCHQ Certified Training (GCT).