

**МИНОБРНАУКИ РОССИИ**  
**Ярославский государственный университет им. П.Г. Демидова**

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

20 июня 2023 г.

**Рабочая программа дисциплины**  
**Основы управления информационной безопасностью**

Направление подготовки (специальности)  
10.03.01 Информационная безопасность

Направленность (профиль)  
«Безопасность компьютерных систем (в сфере информационных технологий)»

Форма обучения очная

Программа рассмотрена  
на заседании кафедры  
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК  
математического факультета  
протокол № 9 от 3 мая 2023 г.

### 1. Цели освоения дисциплины

Целью освоения дисциплины «Основы управления информационной безопасностью» является теоретическая и практическая подготовка к деятельности, связанной с применением методов управления информационной безопасностью объектов информатизации.

### 2. Место дисциплины в структуре ОП

«Основы управления информационной безопасностью» относится к числу дисциплин базовой части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент овладел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – работа с программными средствами общего назначения;

«Теория информации» – знание основ и содержания современных методов получения, обработки, хранения, использования и уничтожения информации.

«Основы информационной безопасности» - знание основ обеспечения информационной безопасности.

Знания и навыки, полученные в результате изучения дисциплины «Основы управления информационной безопасностью», используются студентами в дальнейшем при разработке курсовых и дипломных работ.

### 3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

ОПК-5; ОПК-6; ОПК-10; ОПК-12

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
<b>Общепрофессиональные компетенции</b>		
<b>ОПК- 5</b> Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	<b>И-ОПК-5_1.</b> Знает и понимает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	<b>Знать</b> основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.
	<b>И-ОПК-5_2.</b> Имеет навык применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации	<b>Уметь</b> применять на практике нормативно правовые акты, методические документы, регламентирующие деятельность по защите информации в организации.
	<b>И-ОПК-5_3</b> умеет анализировать и разрабатывать проекты	<b>Уметь</b> разрабатывать проекты локальных НПА по защите информации.

	<p>локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;</p> <p>формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;</p>	
<p><b>ОПК-6</b> Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;</p>	<p><b>И-ОПК-6_1</b> знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях;</p>	<p><b>Знать</b> систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях;</p>
<p><b>ОПК-10</b> Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;</p>	<p><b>И-ОПК-10_3</b> знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности и принципы формирования политики информационной безопасности организации.</p>	<p><b>Знать</b> правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности, и принципы формирования политики информационной безопасности организации.</p> <p><b>Иметь навыки</b> в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.</p>

<b>ОПК-12</b> Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	<b>И-ОПК-12_1</b> знает принципы формирования политики информационной безопасности в информационных системах, принципы организации информационных систем в соответствии с требованиями по защите информации; основные этапы процесса проектирования и общие требования к содержанию проекта	<b>Уметь</b> готовить исходные данные для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;
---	---	---

#### 4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 акад. часа.

Формы текущего контроля успеваемости									
№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	Самостоятельная работа	
1	Цели, задачи и содержание управления информационной безопасностью.	7	4			2			Опрос на практических занятиях
2	Система управления информационной безопасностью автоматизированных систем.	7	6			2		7	Опрос на практических занятиях
3	Политика безопасности предприятия и автоматизированных систем.	7	10	16		2		30	Опрос на практических занятиях
4	Аудит информационной безопасности автоматизированных систем.	7	12	16		2		30	Опрос на практических занятиях
							0,3	4,7	зачет
	Всего	144	32	32		8	0,3	71,7	

#### Содержание разделов дисциплины:

Тема № 1 Цели, задачи и содержание управления информационной безопасностью.

1.1. Введение. Цели, задачи и содержание дисциплины «Основы управления информационной безопасностью». Рекомендуемая литература.

1.2. Основные понятия и определения управления информационной безопасностью.

1.3. Содержание и задачи процесса управления информационной безопасностью объекта информатизации.

Тема № 2 Система управления информационной безопасностью автоматизированных систем.

2.1. Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ в организации.

2.2. Стандартизация в сфере управления ИБ (на основе международных стандартов ISO/IEC 17799, ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 27004, ISO/IEC 27007).

2.3. Краткий обзор стандартов России, связанных с обеспечением и управлением ИБ и созданных на основе «Общих критериев» для выражения национальных интересов Российской Федерации в данной сфере (ГОСТ Р ИСО/МЭК 15408).

2.4. Ресурсы организации, подлежащие защите с точки зрения ИБ.

2.5. Комплекс методов и средств защиты информации как объект управления ИБ.

Тема № 3 Политика безопасности предприятия и автоматизированных систем.

3.1. Назначение и содержание политики ИБ организации в целом, его структурных подразделений, частных политик безопасности. Средства их реализации.

3.2. Модель нарушителя политики безопасности.

3.3. Типичные угрозы информации и уязвимости корпоративных АС.

3.4. Разграничение полномочий и ответственности персонала, обеспечивающего реализацию положений нормативно-распорядительных документов по защите информации организации.

Тема № 4 Аудит информационной безопасности автоматизированных систем.

4.1. Назначение, цели и виды аудита ИБ.

4.2. Требования к аудиту ИБ, особенности взаимодействия между аудитором и заказчиком.

4.3. Оценка работы аудитора.

4.4. Стандартизация в сфере аудита ИБ. Содержание и организация процесса аудита ИБ.

4.5. Оценка рисков ИБ.

4.6. Отчетные документы по результатам аудита.

4.7. Выполнение рекомендаций по итогам проведения аудита ИБ.

## **5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине**

В процессе обучения используются следующие образовательные технологии:

**Вводная лекция** – дает первое целостное представление о дисциплине (или ее разделе) и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки специалиста. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках курса, а также дается анализ рекомендуемой учебно-методической литературы.

**Академическая лекция с элементами лекции-беседы** – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет

привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

**Практическое занятие** – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний по предложенному алгоритму.

**Консультации** – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

**Электронный учебный курс «Основы управления информационной безопасностью» в LMS Электронный университет Moodle ЯрГУ**, в котором:

- представлены задания для самостоятельной работы обучающихся по темам дисциплины;
- осуществляется проведение отдельных мероприятий текущего контроля успеваемости студентов;
- представлены тексты лекций по отдельным темам дисциплины;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;

посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

#### **6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине**

В процессе осуществления образовательного процесса по дисциплине используются: для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- Adobe Acrobat Reader;
- Интернет-версия справочной системы Гарант.

#### **7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)**

В процессе осуществления образовательного процесса по дисциплине используются: Автоматизированная библиотечно-информационная система «БУКИ-NEXT»  
[http://www.lib.uni-yar.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uni-yar.ac.ru/opac/bk_cat_find.php)

#### **8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

##### **а) основная литература**

1. Проскурин В.Г., «Защита программ и данных», 2-е издание, учебное пособие для студ. учреждений высш. проф. образования, М., Издательский центр «Академия», 2012.- 208с

2. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 5 декабря 2016г. № 646).
3. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ.
4. Курило, А. П. Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Вып. 1. - Москва : Горячая линия - Телеком, 2013. - 244 с. (Серия "Вопросы управления информационной безопасностью".) - ISBN 978-5-9912-0271-8. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785991202718.html> (дата обращения: 29.01.2022). - Режим доступа : по подписке.
5. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учебное пособие для вузов / Милославская Н. Г. , Сенаторов М. Ю. , Толстой А. И. - Вып. 4. - Москва : Горячая линия - Телеком, 2013. - 216 с. (Серия "Вопросы управления информационной безопасностью") - ISBN 978-5-9912-0274-9. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785991202749.html> (дата обращения: 29.01.2022). - Режим доступа : по подписке.

#### **б) дополнительная литература**

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/491249> (дата обращения: 29.01.2022).
2. Белов, Е. В. Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва : Горячая линия - Телеком, 2011. - 544 с. - ISBN 5-93517-292-5. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN5935172925.html> (дата обращения: 29.01.2022). - Режим доступа : по подписке.
3. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/114688> (дата обращения: 29.01.2022). — Режим доступа: для авториз. пользователей.
4. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / Шаньгин В. Ф. - Москва : ДМК Пресс, 2012. - 592 с. - ISBN 978-5-94074-637-9. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785940746379.html> (дата обращения: 29.01.2022). - Режим доступа : по подписке
5. ГОСТ Р ИСО/МЭК 56045-2014г., «Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью». Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2015. - 44с.
6. ГОСТ Р ИСО/МЭК ТО 19791-2008г., «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2009. - 126с.
7. ГОСТ Р ИСО/МЭК 27007-2014г., «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2015. - 27с.
8. ГОСТ Р ИСО/МЭК 18044-2007г., «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»,

Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2009. - 46с.

9. ГОСТ Р ИСО/МЭК 18045-2013г., «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2014. - 250с.

10. ГОСТ Р ИСО/МЭК 53131-2008 «Защита информации. Рекомендации по услугам восстановления информации после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2011. - 48с.

11. ГОСТ Р ИСО/МЭК 15408-1-2012г., 15408-2-2013г., 15408-3-2013г., «Информационная технология. Методы и средства обеспечения информационной безопасности. Критерии оценки безопасности информационных технологий», «Часть 1. Введение и общая модель», «Часть 2. Функциональные компоненты безопасности», «Часть 3. Компоненты доверия к безопасности», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», Часть 1.-2014.-56с., Часть 2.-2014.-164с., Часть 3.-2014.-152с.

12. Информационный документ ФСТЭК России № 240/24/3095 от 20.03.2012г. «об утверждении Требований к средствам антивирусной защиты». ФСТЭК России, 2012.-3с.

13. Руководящий документ ФСТЭК России (бывш. Гостехкомиссия) «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей». (утв. решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г., № 114).

#### **в) ресурсы сети «Интернет»**

1. Официальный сайт Центра по лицензированию, сертификации и защите государственной тайны ФСБ России. Перечень средств защиты информации, сертифицированных ФСБ России. (<http://clsz.fsb.ru/certification.htm>).

2. Официальный сайт Федеральной службы по техническому и экспортному контролю (<http://fstec.ru/>).

3. Электронная библиотека учебных материалов ЯрГУ: ([http://www.lib.uni-yar.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uni-yar.ac.ru/opac/bk_cat_find.php)).

4. Информационная система «Единое окно доступа к образовательным ресурсам»: (<http://www.edu.ru> (раздел Учебно-методическая библиотека) или по прямой ссылке: <http://window.edu.ru/library>).

5. Новости в сфере угроз безопасности и защиты компьютерной информации российских журнала «Хакер»: <https://xakep.ru/tag/news> и журнала «Информационная безопасность»: <http://itsec.ru/main.php>.

6. Новейшие данные об угрозах работы с подключением к сети Интернет российской компании «Лаборатория Касперского»: <http://www.kaspersky.ru/internet-security-center>.

#### **9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.**

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;



- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:

старший преподаватель кафедры КБ и ММОИ А.В. Саханда

**Приложение № 1 к рабочей программе дисциплины  
«Основы управления информационной безопасностью»**

**Фонд оценочных средств  
для проведения текущей и промежуточной аттестации студентов  
по дисциплине**

**1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

**1.1 Контрольные задания и иные материалы,  
используемые в процессе текущей аттестации**

**Перечень вопросов для опросов на практических занятиях:**

**Вопросы по теме 1.**

1. Как определяется понятие системы?
2. Каковы основные свойства системы?
3. В чем заключается системный подход к исследованию объектов?
4. Каковы особенности рассмотрения системного подхода применительно к управлению?
5. Какие элементы процесса могут быть исключены из определения: входные данные процесса, выходные данные процесса, управляющее воздействие, ресурсы?
6. Какие виды деятельности в организации можно назвать процессом (или бизнес-процессом)?
7. Какую роль играют процессы в терминах системного подхода к организации?
8. Кто в организации может и должен определить цели бизнес-процессов?
9. Что понимается под ресурсами в рамках определения понятия процесса?
10. Что понимается под управляющим воздействием в рамках определения понятия процесса?
11. В чем заключается процессный подход?
12. Дайте определение понятия «управление» с позиций системного подхода.
13. Дайте определение понятия «менеджмент».
14. В чем отличия понятий «управление» и «менеджмент»?
15. Каковы основные функции управления?
16. Что такое метод управления?
17. Что такое система управления?
18. Что такое система управления, основанная на процессном подходе?
19. Каковы особенности рассмотрения процессного подхода применительно к управлению?
20. К каким процессам организации может быть применена циклическая модель PDCA?
21. В чем состоят основные преимущества использования циклической модели PDCA?
22. В чем отличие терминов «защита информации» и «информационная безопасность»?
23. Какие свойства ИБ в современных условиях должны приниматься во внимание? Поясните, что понимается под каждым из свойств.

**Вопросы по теме 2.**

1. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

2. Для организаций какой сферы применимы стандарты серии ISO/IEC 27000?
3. Каковы отличительные черты серии стандартов ISO/IEC 27000?
4. Какой из стандартов серии ISO/IEC 27000 содержит требования к созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?
5. В чем состоят основные различия и сходства стандартов ISO/IEC 27001 и ITU-T X.1051?
6. Какой из стандартов серии ISO/IEC 27000 признан каталогом «лучших» практик по ИБ?
7. В каком стандарте серии ISO/IEC 27000 содержится руководство по внедрению СУИБ?
8. На основании чего может проводиться оценка эффективности СУИБ?
9. Можно ли проводить аудит (или сертификацию) на соответствие стандарту ISO/IEC 27002 (бывший ISO/IEC 17799)?
10. Каковы основные идеи руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ?
11. Почему подход к проведению аудитов систем менеджмента качества и окружающей среды, изложенный в стандарте ISO/IEC 19011, может быть применен для проведения внутренних аудитов СУИБ?
12. В каком стандарте серии ISO/IEC 27000 описана инфраструктура руководства ИБ?
13. Какой стандарт серии ISO/IEC 27000 рассматривает вопросы управления безопасностью сетей?
14. В чем состоят преимущества использования (учета) требований российских и международных стандартов по управлению ИБ при построении СУИБ или отдельных процессов управления ИБ?
15. Каковы преимущества одновременного учета требований стандартов, предъявляемых как к СУИБ в целом, так и стандартов, предъявляющих требования к отдельным процессам, разрабатываемым в рамках СУИБ?
16. В чем состоят основные сходства и различия между стандартами на СУИБ и на отдельные процессы управления ИБ?
17. Какие методы и средства ОИБ для ИТ рассматриваются в стандартах ISO/IEC 13335 и идентичных им ГОСТ Р ИСО/МЭК 13335?
18. Как оценивается ИБ ИТ согласно стандартам ISO/IEC 15408 и 18045 и идентичных им ГОСТ Р ИСО/МЭК?
19. Какие из рассмотренных стандартов затрагивают аспекты анализа рисков ИБ?
20. Каковы основные цели построения системы УИБ, соответствующей требованиям стандартов BS 25999 и 25777?
21. В чем может заключаться различие между требованиями к системам управления непрерывностью бизнеса и к процессу управления непрерывностью бизнеса?
22. Каковы основные цели следования модели PDCA при построении процесса управления инцидентами ИБ в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?
23. Какие тенденции характерны для развития стандартизации управления ИБ в Российской Федерации (на примере итераций ГОСТ Р ИСО/МЭК 15408-1-2012г., 15408-2-2013г., 15408-3-2013г., «Информационная технология. Методы и средства обеспечения информационной безопасности. Критерии оценки безопасности информационных технологий», «Часть 1. Введение и общая модель», «Часть 2. Функциональные компоненты безопасности», «Часть 3. Компоненты доверия к безопасности»)?
24. На базе анализа ГОСТ Р ИСО/МЭК 15408-1-2012г., 15408-2-2013г. «Информационная технология. Методы и средства обеспечения информационной безопасности. Критерии оценки безопасности информационных технологий», «Часть 1. Введение и общая модель», «Часть 2. Функциональные компоненты безопасности»,

сформулируйте основные компоненты парадигмы функциональных компонентов безопасности ИТ?

25. На базе анализа ГОСТ Р ИСО/МЭК 15408-1-2012г., 15408-3-2013г., «Информационная технология. Методы и средства обеспечения информационной безопасности. Критерии оценки безопасности информационных технологий», «Часть 1. Введение и общая модель», «Часть. 3. Компоненты доверия к безопасности», сформулируйте основные компоненты парадигмы компонентов доверия безопасности ИТ?

24. В чем состоят преимущества использования «отраслевых» стандартов на СУИБ по сравнению, например, со стандартом ISO/IEC 27001, требования которого применимы к любой организации независимо от отрасли или сферы деятельности?

25. Каково значение стандартов серии СТО БР ИББС в рамках развития стандартизации управления ИБ в России?

26. Какие аспекты регламентируют стандарты серии СТО БР ИББС, если говорить об управлении ИБ?

27. Каковы основные цели и задачи стандартизации по ОИБ организаций БС РФ?

28. Каковы основные цели проведения аудита ИБ организаций БС РФ?

29. Какова цель и направленность российских стандартов в сфере обеспечения компьютерной безопасности, разработанных в дополнение «Общих критериев»?

30. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 19791-2008.

31. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 51583-2014.

32. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 15446-2008.

33. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 52447-2005.

34. Охарактеризуйте содержание российских стандартов ГОСТ Р ИСО/МЭК 53113.1-2008 и 53113.2-2009.

35. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 53115-2008.

36. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 53131-2008.

37. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 27034-1-2014.

38. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 56824-2015.

39. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 56545-2015.

40. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 56546-2015.

44. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 27007-2014г., «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности».

### **Вопросы по теме 3.**

1. Какие определения ПолиБ даются в различных международных стандартах?
2. В чем различие политик, стандартов, правил и процедур ОИБ?
3. Что такое трастовые модели?
4. С каких точек зрения и как можно описать виды ПолиБ?
5. Что понимают под ПолиБ в широком и узком смыслах?

6. Для чего разрабатываются организационные (административные) и технические ПолИБ?
7. Перечислите основные требования, предъявляемые в различных источниках к ПолИБ?
8. Каковы основные принципы, позволяющие разработать эффективную ПолИБ?
9. Каково содержание документа, описывающего корпоративную ПолИБ? Что излагается в каждом из разделов этой политики?
10. Назовите типовые цели корпоративной ПолИБ.
11. Каковы отличительные особенности содержания частной ПолИБ для отдельной области, требующей ОИБ, и для отдельной системы, используемой в организации? Что общего между этими политиками? Что излагается в каждом из разделов этих политик?
12. Назовите основные стадии жизненного цикла ПолИБ? Из каких шагов они состоят? Какие из этих шагов выполняются итерационно и почему?
13. Отдельно сформулируйте цель и основные мероприятия, осуществляемые на каждом шаге жизненного цикла ПолИБ.
14. Как происходит процесс информирования в отношении ПолИБ?
15. Для чего и кем осуществляются ревизия, мониторинг и аудит ПолИБ? В чем отличия этих шагов жизненного цикла ПолИБ?
16. Что понимается под исключениями из ПолИБ?
17. Зачем необходим пересмотр ПолИБ?
18. В каких случаях ПолИБ может быть аннулирована?
19. Что такое «роль»? Какие роли связаны с использованием ПолИБ?
20. Какие виды ответственности связаны со всеми стадиями жизненного цикла ПолИБ?
21. Какими принципами необходимо руководствоваться при установлении ответственности в отношении соблюдения ПолИБ?
22. Дайте определения «ОИБ», «управления ИБ» и «СУИБ» организации.
23. Опишите деятельность по ОИБ организации как процесс. Каковы его входные и выходные данные, ресурсы и управляющие воздействия?
24. Как процесс ОИБ в организации связан с процессами основной деятельности организации?
25. Каковы основные этапы процесса управления ИБ ИТТ?
26. Что является хорошей практикой при выборе области действия СУИБ? Какие стратегии выбора области действия СУИБ существуют?
27. Какие факторы необходимо учитывать при выборе области действия СУИБ?
28. Какие параметры процессов являются наиболее значимыми при выборе области действия проектируемой СУИБ?
29. Что входит в документальное обеспечение СУИБ? Каковы этапы его жизненного цикла?
30. Какие уровни документов включает в себя иерархия документов СУИБ? Какие виды конкретных документов создаются на каждом из уровней?
31. В чем состоит основное отличие между понятиями документ и запись?
32. В чем заключается процесс управления документами и записями?
33. Какова взаимосвязь между понятиями ПолИБ и Политика СУИБ?
34. Что должна включать в себя Политика СУИБ?
35. На каких этапах руководство организации должно продемонстрировать свою приверженность к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?
36. В чем состоит основная необходимость участия высшего руководства в жизненном цикле СУИБ?

37. Каким образом при использовании циклической модели PDCA применительно к СУИБ требования и ожидания к результатам ОИБ преобразуются в управляемую ИБ?
38. Дайте определение «процесс управления ИБ» организации.
39. Какие действия и процессы выполняются на стадии планирования СУИБ? Каковы задачи данного этапа?
40. Специалистов каких подразделений необходимо включать в рабочую группу по построению СУИБ и почему?
41. Какие действия и процессы выполняются на стадии реализации и внедрения СУИБ? Каковы задачи данного этапа?
42. Какие действия и процессы выполняются на стадии проверки СУИБ? Каковы задачи данного этапа?
43. Какие действия и процессы выполняются на стадии совершенствования СУИБ? Каковы задачи данного этапа?
44. В чем разница и сходство между понятиями корректирующего и предупреждающего действий?
45. Почему в рамках процессного подхода к управлению ИБ следует особое внимание уделять мониторингу и анализу результативности и эффективности СУИБ?
46. В чем состоят различия между основными свойствами процессов: эффективность и результативность?
47. Что входит в понятие «задание процесса управления ИБ»?
48. Какие этапы включает в себя идентификация процессов управления ИБ в организации и какие действия необходимо предпринять в рамках этих этапов?
49. Каковы основные преимущества документирования процессов управления ИБ организации и наличия подробных карт процессов организации?
50. Каковы основные элементы процесса мониторинга процессов управления ИБ организации?
51. На основе каких данных необходимо разрабатывать метрики мониторинга для процессов управления ИБ?
52. На что может указывать расхождение между целевым и текущим значениями метрик мониторинга для процессов управления ИБ?
53. Какая информация может потребоваться для того, чтобы определить целевое значение метрик процесса управления ИБ и кто может предоставить такую информацию?
54. Какой тип процессов управления ИБ представляет наибольший интерес для анализа и мониторинга при эксплуатации СУИБ?
55. Возможно ли построение СУИБ, охватывающей несколько территориальных подразделений организации? Какие особенности при этом необходимо учитывать?
56. В чем состоят основные преимущества и недостатки стратегии построения и внедрения СУИБ в целом?
57. В чем состоят основные преимущества и недостатки стратегии построения и внедрения отдельных процессов управления ИБ с последующим их объединением в СУИБ?
58. Какова предпочтительная последовательность внедрения процессов управления ИБ?
59. В чем состоят преимущества и недостатки построения СУИБ для небольшой области действия с возможным расширением в будущем?
60. В чем состоят преимущества и недостатки построения СУИБ для большой области действия?
61. Какой вид управления необходим при построении единой СУИБ, распространяющейся на несколько территориальных подразделений организации?
62. Наличие каких ролей необходимо в рамках ролевой структуры СУИБ?
63. В чем состоит преимущество использования ролевого принципа в рамках СУИБ?

#### Вопросы по теме 4

1. Какие виды проверок СУИБ существуют? Каковы их основные цели и результаты (в сравнении)?
  2. Как взаимосвязаны понятия аудита и мониторинга ИБ?
  3. На основе каких документов осуществляется проверка и оценка СУИБ?
  4. Каковы направления оценки ИБ? Как эти направления связаны с СУИБ?
  5. Что понимают под мониторингом ИБ? Каковы его цели?
  6. Назовите процессы мониторинга ИБ и конкретные основные действия соответствующих ответственных лиц.
  7. Какая важная с точки зрения обеспечения ИБ информация содержится в журналах регистрации событий?
  8. Рассмотрите структуру СОВ как динамических средств мониторинга ИБ.
  9. Определите понятие «самооценка ИБ».
  10. Каковы преимущества для организации в проведении самооценки ИБ?
  11. Опишите основные этапы проведения самооценки ИБ.
  12. Что отражается в отчете о проведенной самооценке ИБ?
  13. Какие различают виды аудитов ИБ? В чем их сходство и различия?
  14. Каковы преимущества внутренних аудитов ИБ перед внешними?
  15. Перечислите цели и задачи внутренних аудитов ИБ.
  16. Назовите и поясните организационные принципы и принципы эффективности внутреннего аудита ИБ.
  17. Рассмотрите деятельность подразделения внутреннего аудита организации, контролирующего вопросы ИБ.
  18. Что такое «внешний аудит ИБ»? Какие выделяют виды этих аудитов согласно различным стандартам?
  19. На чем в первую очередь должен сосредоточиться внешний аудит ИБ?
  20. Определите принципы проведения внешнего аудита ИБ.
  21. Как осуществляется управление программой внешнего аудита ИБ?
  22. Каковы цели и задачи программы внешнего аудита ИБ?
  23. Рассмотрите этапы управления программой внешних аудитов ИБ в рамках цикла PDCA.
  24. От каких факторов зависит объем программы внешнего аудита ИБ?
  25. Какие этапы включают работы по проведению внешнего аудита ИБ?
- Подробно остановитесь на каждом из этапов.
26. Какие документы анализируются внешними аудиторами ИБ? Приведите в качестве примера анализ документации при аудите ИБ ИС.
  27. Как осуществляется планирование аудитов ИБ: входные данные, аспекты, требующие особого внимания? Что ходит в план аудита ИБ и кто его готовит?
  28. Как проводится внешний аудит на месте?
  29. Какие свидетельства аудита ИБ собираются, каким образом и каковы приоритеты их достоверности?
  30. Что отражается в отчете по внешнему аудиту ИБ?
  31. Что включают в себя требования к компетентности и опыту аудиторов ИБ? Что они должны знать и уметь в различных областях знаний, применяемых при внешнем аудите ИБ?
  32. Как во время внешнего аудита ИБ осуществляется взаимодействие между аудиторской группой и проверяемой организацией? Кто и за что несет ответственность?
  33. Какова роль высшего руководства в процессе проверок СУИБ?
  34. На основе каких документов осуществляется анализ СУИБ со стороны руководства организации?

35. Каково основное назначение процессов управления корректирующими и предупреждающими действиями?
36. Что понимают под тактическими и стратегическими улучшениями СУИБ?
37. Какие методы тестирования в информационной среде применимы при различных проверках ИБ?
38. Какие инструментальные средства используются при проверках и оценках ИБ?
39. В чем отличие понятий «эффективность» и «результативность» применительно к СУИБ?
40. Какие показатели используются для оценки эффективности СУИБ?
41. Определите понятия «измерение», «показатель» и «метрика» и укажите их различия.
42. Что понимают под метрикой безопасности? Для чего используются метрики безопасности? Каково их основное назначение?
43. Какими должны быть метрики безопасности?
44. Рассмотрите основные этапы процесса выработки программы получения метрик безопасности.
45. Какие подходы используются при выработке метрик безопасности?
46. Какие метрики безопасности предлагаются организацией Center for Internet Security для управления инцидентами ИБ, уязвимостями, обновлениями, конфигурациями, изменениями и защиты приложений?
47. На примере управления инцидентами ИБ перечислите основные атрибуты и покажите, как рассчитываются метрики безопасности.
48. Чему посвящен стандарт ИСО/МЭК 27004:2009?
49. Какие факторы должны быть учтены при определении целей проведения измерений для СУИБ?
50. Как связаны измерения с моделью PDCA для СУИБ?
51. Какая модель измерений, связанных с ИБ, положена в основу стандартов ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011?
52. Что такое основная и производная меры измерений и показатели? Как они получаются?
53. Что понимается под методом измерения, функцией измерений и аналитической моделью согласно ISO/ШС 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011?
54. Какие критерии принятия решений могут быть установлены для показателей?
55. Как определяются информационные потребности согласно ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011?
56. Основываясь на ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011, составьте описание конструктивных элементов измерения для анализа лог- файлов и защиты от вредоносного ПО.
57. Как и с какими целями производится оценка зрелости процессов управления ИБ?
58. Сколько уровней зрелости можно выделить для процессов управления ИБ в соответствии с различными международными подходами и стандартами?
59. Что может потребоваться для достижения четвертого уровня (или выше) зрелости процесса управления ИБ или системы процессов?
60. Что показывает зрелость процесса СУИБ?



## **1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации**

### **Список вопросов к зачету**

1. Перечислите и охарактеризуйте угрозы информационной безопасности Российской Федерации, указанные в «Доктрины информационной безопасности» Российской Федерации.
2. Назовите и опишите цели, задачи и направленность «Доктрины информационной безопасности» Российской Федерации.
3. Сформулируйте и обоснуйте общие принципы построения защиты информации в России.
4. В чем суть российской классификация угроз и ее отличие от принятой в западных стандартах.
5. Охарактеризуйте систему управления, основанная на процессном подходе.
6. Каковы особенности рассмотрения процессного подхода применительно к управлению? Дайте развернутое объяснение.
7. К каким процессам организации может быть применена циклическая модель PDCA?
8. Дайте развернутое определение понятия «управление» с позиций системного подхода.
9. Какие свойства ИБ в современных условиях должны приниматься во внимание? Поясните, что понимается под каждым из свойств.
10. Приведите требования к созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?
11. Расскажите и поясните, - в чем состоят преимущества использования (учета) требований российских и международных стандартов по управлению ИБ при построении СУИБ или отдельных процессов управления ИБ?
12. Каковы преимущества одновременного учета требований стандартов, предъявляемых как к СУИБ в целом, так и стандартов, предъявляющих требования к отдельным процессам, разрабатываемым в рамках СУИБ?
13. Какие и как российские стандарты затрагивают аспекты анализа рисков ИБ?
14. Поясните развернуто различие между требованиями к системам управления непрерывностью бизнеса и к процессу управления непрерывностью бизнеса?
15. Приведите и поясните основные цели следования модели PDCA при построении процесса управления инцидентами ИБ в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?
16. Назовите и охарактеризуйте тенденции характерные для развития стандартизации управления ИБ в Российской Федерации.
17. Укажите цель и направленность российских стандартов в сфере обеспечения компьютерной безопасности, разработанных в дополнение «Общих критериев».
18. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 19791-2008.
19. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 51583-2014.
20. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 15446-2008.
21. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 52447-2005.
22. Охарактеризуйте содержание российских стандартов ГОСТ Р ИСО/МЭК 53113.1-2008 и 53113.2-2009.
23. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 53115-2008.

24. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 53131-2008.
25. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 27034-1-2014.
26. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 56824-2015.
27. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 56545-2015.
28. Охарактеризуйте содержание российского стандарта ГОСТ Р ИСО/МЭК 56546-2015.
29. Требования и принципы, учитываемые при разработке политики информационной безопасности.
30. Содержание политики информационной безопасности организации.
31. Система управления информационной безопасностью организации.
32. Процессный подход к управлению информационной безопасностью организации.
33. Работа с процессами системы управления информационной безопасностью организации.
34. Стратегии построения и внедрения системы управления информационной безопасностью организации.
35. Системный подход к управлению рисками информационной безопасности.
36. Установление контекста управления рисками информационной безопасности.
37. Содержание двух этапов оценки рисков информационной безопасности.
38. Содержание оценки и анализа рисков информационной безопасности. Обработка рисков.
39. Понятие, коммутация, мониторинг и пересмотр рисков информационной безопасности.
40. Обеспечение управления рисками информационной безопасности организации.
41. Управление инцидентами информационной безопасности организации.
42. Управление непрерывностью бизнеса организации.
43. Рассмотрите деятельность подразделения внутреннего аудита организации, контролирующего вопросы ИБ.
44. Что такое «внешний аудит ИБ»? Какие выделяют виды этих аудитов согласно различным стандартам? На чем в первую очередь должен сосредоточиться внешний аудит ИБ? Определите принципы проведения внешнего аудита ИБ.
45. Каковы цели и задачи программы внешнего аудита ИБ? От каких факторов зависит объем программы внешнего аудита ИБ? Обоснуйте и сформулируйте этапы управления программой внешних аудитов ИБ в рамках цикла PDCA.
46. Какие этапы включают работы по проведению внешнего аудита ИБ? Подробно остановитесь на каждом из этапов. Какие документы анализируются внешними аудиторами ИБ и почему? Как проводится внешний аудит на месте? Какие свидетельства аудита ИБ собираются, каким образом и каковы приоритеты их достоверности? Что отражается в отчете по внешнему аудиту ИБ?
47. На основе каких документов осуществляется анализ СУИБ со стороны руководства организации? Каково основное назначение процессов управления корректирующими и предупреждающими действиями со стороны руководства проверяемой организации?
48. Что понимают под тактическими и стратегическими улучшениями СУИБ? Какие методы тестирования в информационной среде применимы при различных проверках ИБ? Какие инструментальные средства используются при проверках и оценках ИБ?
49. Какие подходы используются при выработке метрик безопасности. Какие показатели используются для оценки эффективности СУИБ? На произвольном примере

управления инцидентами ИБ перечислите основные атрибуты и покажите, как рассчитываются метрики безопасности.

50. Как и с какими целями производится оценка зрелости процессов управления ИБ? Сколько уровней зрелости можно выделить для процессов управления ИБ в соответствии с различными международными подходами и стандартами? Охарактеризуйте, - что показывает зрелость процесса СУИБ?

## **2. Правила приема зачета.**

Оценка знаний по итогу прохождения курса проводится в форме принятия зачета.

На зачете проверяется сформированность всех указанных в учебной программе компетенций.

В билет для зачета включаются два теоретических вопроса. На подготовку к ответу дается не менее 1 академического часа.

Также есть возможность ответить на контрольные вопросы в электронном курсе «Основы управления информационной безопасностью» в LMS Электронный университет Moodle ЯрГУ.

По итогам ответов студенту выставляется одна из оценок: «зачтено», «не зачтено».

**Оценка «зачтено»** выставляется студенту, если: он знает основные определения, последователен в изложении материала, демонстрирует базовые знания дисциплины, владеет необходимыми умениями и навыками при выполнении практических заданий.

**Оценка «не зачтено»** выставляется студенту, если: он не знает основных определений, непоследователен и сбивчив в изложении материала, не обладает определенной системой знаний по дисциплине, не в полной мере владеет необходимыми умениями и навыками при выполнении практических заданий.

**Оценка «не зачтено»** выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

## **Приложение №2 к рабочей программе дисциплины «Основы управления информационной безопасностью»**

### **Методические указания для студентов по освоению дисциплины**

Изучение дисциплины предполагает уверенное владение компьютером, умение осуществлять поиск и оценку достоверности необходимой информации в сети Интернет, но студенту достаточно сложно самостоятельно освоить вопросы дисциплины «Основы управления информационной безопасностью». Посещение всех предусмотренных аудиторных занятий является совершенно необходимым в силу обучения на них учащихся сравнительным оценкам знаний из различных источников, критической их оценки. Также без упорных и регулярных самостоятельных занятий в течение семестра, желательно с «упреждающим знакомством» с содержанием предстоящего занятия, крайне сложно усвоить логику и аргументацию упомянутых сравнительных оценок и критического анализа знаний из различных источников, что не позволит студентам развить продвинутого и высокого уровня компетенций.

### **Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине**

Для самостоятельной работы рекомендуется использовать учебную литературу, интернет-источники, указанные в разделе 8 настоящей Рабочей программы и электронный курс «Основы управления информационной безопасностью» в LMS Электронный университет Moodle ЯрГУ.