Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
# **Основы управления информационной безопасностью**

Образовательная программа: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Курс: 4, семестр : 7

Факультет автоматики и вычислительной техники,

| | | **Семестр** |
|---|---|---|
| **№** | **Вид деятельности** | **7** |
| **1** | Всего зачетных единиц (кредитов) | 5 |
| **2** | Всего часов | 180 |
| **3** | Всего занятий в контактной форме, час. | 69 |
| **4** | Лекции, час. | 36 |
| **5** | Практические занятия, час. | 18 |
| **6** | Лабораторные занятия, час. | |
| **7** | из них в активной и интерактивной форме, час. | 18 |
| **8** | Аттестация, час. | 2 |
| **9** | Консультации, час. | 13 |
| **10** | Самостоятельная работа, час. | 111 |
| **11** | Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе) | РГЗ |
| **12** | Вид аттестации | Э |

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.03.01 Информационная безопасность

ФГОС введен в действие приказом №1515 от 01.12.2016 г. , дата утверждения: 20.12.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, базовая

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.03.01 Информационная безопасность

Рабочая программа обсуждена на заседании кафедры

ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

старший преподаватель, Дронова Г. А.

Заведующий кафедрой:

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

заведующий кафедрой Трушин В. А.

## 1. Внешние требования

Таблица 1.1

| |
|---|
| ***Компетенция ФГОС*: ОК.2 способность использовать основы экономических знаний в различных сферах деятельности; *в части следующих результатов обучения*:** |
| у4. уметь оценивать управление предприятием с позиции внутреннего состояния и внешнего окружения |
| ***Компетенция ФГОС*: ПК.13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации; *в части следующих результатов обучения*:** |
| з1. знать основные методы управления информационной безопасностью |
| ***Компетенция ФГОС*: ПК.6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; *в части следующих результатов обучения*:** |
| у1. уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем |

## 2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

| Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть) | Формы организации занятий |
|---|---|
| *Основы управления информационной безопасностью* | |
| **ОК.2.у4 уметь оценивать управление предприятием с позиции внутреннего состояния и внешнего окружения** | |
| **1**.уметь оценивать управление предприятием с позиции внутреннего состояния и внешнего окружения | Лекции; Практические занятия; Самостоятельная работа |
| **ПК.6.у1 уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем** | |
| **2**.уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем | Лекции; Практические занятия; Самостоятельная работа |
| **ПК.13.з1 знать основные методы управления информационной безопасностью** | |
| **3**.знать основные методы управления информационной безопасностью | Лекции; Практические занятия; Самостоятельная работа |

## 3. Содержание и структура учебной дисциплины

Таблица 3.1

| Темы лекций | Активные формы, час. | Часы | Ссылки на результаты обучения | Учебная деятельность |
|---|---|---|---|---|
| **Семестр: 7** | | | | |
| **Дидактическая единица: Система обеспечения ИБ как совокупность системы ИБ и системы управления ИБ.** | | | | |
| 1. Система обеспечения ИБ как совокупность системы ИБ и системы управления ИБ. Цикл Демминга. Процессный подход к ИБ. Составляющие процесса. Оценка результативности процесса. Метрики. Уровни зрелости процессов | 0 | 4 | 1 | |
| **Дидактическая единица: Информационные ресурсы организации.** | | | | |

| | | | | |
|---|---|---|---|---|
| 2. Информационные ресурсы организации. Типы ИР. Информационные активы и пассивы. Категорирование ИР. Классификация ИР по требованиям закона ФЗ-152 | 0 | 4 | 1 | |
| **Дидактическая единица: Модель угроз и модель нарушителя.** | | | | |
| 3. Модель угроз и модель нарушителя. Понятие. Образцы. Пример разработки | 0 | 4 | 1, 2 | |
| **Дидактическая единица: Процесс Управление рисками ИБ.** | | | | |
| 4. Процесс Управление рисками ИБ. Определение уязвимостей информационных ресурсов, вероятности реализации угроз и возможных финансовых потерь. Понятие риска ИБ. Методы управления рисками ИБ | 0 | 4 | 2 | |
| **Дидактическая единица: Процесс ИБ Управления инцидентами, его связь с ИТ-процессами** | | | | |
| 5. Процесс ИБ Управления инцидентами, его связь с ИТ-процессами Управления проблемами и Управление конфигурацией. Расследование компьютерных инцидентов. Системы учета. ЗНО, ЗНИ, ЗНП | 0 | 4 | | Процесс ИБ Управления инцидентами, его связь с ИТ-процессами Управления проблемами и Управление конфигурацией. Расследование компьютерных инцидентов. Системы учета. ЗНО, ЗНИ, ЗНП |
| **Дидактическая единица: Процессы информационной безопасности, составляющие СУИБ организации.** | | | | |
| 3. Процессы информационной безопасности, составляющие СУИБ организации (18 процессов). Порядок внедрения в деятельность организации | 0 | 4 | 2 | |
| **Дидактическая единица: Процессы информационных технологий.** | | | | |
| 6. Процессы информационных технологий (37 процессов). Общие понятия. Связь с процессами ИБ. ИТ-контроли | 0 | 4 | 3 | |
| **Дидактическая единица: Разработка и внедрение СУИБ на основе процессов ИБ** | | | | |
| 7. Разработка и внедрение СУИБ на основе процессов ИБ. | 0 | 2 | 3 | |
| 8. Аудит и мониторинг СУИБ. Понятие big-date. Применение agile технологий | 0 | 2 | 3 | |
| **Дидактическая единица: Технические системы защиты информации.** | | | | |
| 9. Технические системы защиты информации. Классификация. Применение технических систем в разрезе процессного понимания СУИБ организации. Контроль использования технических систем | 0 | 4 | 3 | |

Таблица 3.2

| Темы практических занятий | Активные формы, час. | Часы | Ссылки на результаты обучения | Учебная деятельность |
|---|---|---|---|---|
| **Семестр: 7** | | | | |
| **Дидактическая единица: Информационные ресурсы организации.** | | | | |
| 1. Разработка мероприятий и проведение процедур категорирования ИР и классификации ИСПДн типовой организации | 4 | 4 | 1 | Разработка мероприятий и проведение процедур категорирования ИР и классификации ИСПДн типовой организации |
| **Дидактическая единица: Процесс Управление рисками ИБ.** | | | | |
| 2. Оценка рисков ИБ типовой организации. Разработка методов управления рисками типовой организации | 2 | 2 | 1 | Оценка рисков ИБ типовой организации. Разработка методов управления рисками типовой организации |
| **Дидактическая единица: Процессы информационной безопасности, составляющие СУИБ организации.** | | | | |
| 3. Процессы информационной безопасности, составляющие СУИБ организации (18 процессов). | 4 | 4 | 1, 2, 3 | Процессы информационной безопасности, составляющие СУИБ организации (18 процессов). Порядок внедрения в деятельность организации |
| **Дидактическая единица: Процессы информационных технологий.** | | | | |
| 4. Процессы информационных технологий (37 процессов). Общие понятия. Связь с процессами ИБ. ИТ-контроли | 4 | 4 | 2, 3 | Процессы информационных технологий (37 процессов). Общие понятия. Связь с процессами ИБ. ИТ-контроли |
| **Дидактическая единица: Разработка и внедрение СУИБ на основе процессов ИБ** | | | | |
| 5. Аудит и мониторинг СУИБ. Понятие big-date. Применение agile технологий | 4 | 4 | 2, 3 | Аудит и мониторинг СУИБ. Понятие big-date. Применение agile технологий |

## 4. Самостоятельная работа обучающегося

| № | Виды самостоятельной работы | Ссылки на результаты обучения | Часы на выполнение | Часы на консультации |
|---|---|---|---|---|
| **Семестр: 7** | | | | |
| 1 | РГЗ | 1, 2, 3 | 42 | 5 |
| : Курлаев С. А. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие / А. С. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000162258. - Загл. с экрана. | | | | |
| 2 | Подготовка к занятиям | 1, 3 | 31 | 3 |
| : Курлаев С. А. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие / А. С. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000162258. - Загл. с экрана. | | | | |
| 3 | Подготовка к аттестации | 1, 2, 3 | 38 | 5 |
| : Курлаев С. А. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие / А. С. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000162258. - Загл. с экрана. | | | | |

## 5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

| Деятельность | Информационно-коммуникационные технологии |
|---|---|
| Информирование | e-mail; Социальные сети |
| Консультирование | e-mail |

## 6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

| Оцениваемые виды деятельности обучающихся | Мин. балл | Максимальный балл |
|---|---|---|
| **Семестр: 7** | | |
| *РГЗ:* | 20 | 40 |
| Контролирующие материалы приводятся в "Дронова Г. А. Управление информационной безопасностью : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 23, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234012" | | |
| *Экзамен:* | 20 | 60 |
| Контролирующие материалы приводятся в "Дронова Г. А. Управление информационной безопасностью : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 23, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234012" | | |

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

| Коды компетенций ФГОС | Результаты обучения | Формы контроля | |
|---|---|---|---|
| | | Защита РГЗ | Экзамен |
| **ОК.2** | у4. уметь оценивать управление предприятием с позиции внутреннего состояния и внешнего окружения | + | + |
| **ПК.13** | з1. знать основные методы управления информационной безопасностью | + | + |
| **ПК.6** | у1. уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем | + | + |

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

## 7. Литература

*Основная литература*

**1.** Романов О. А. Организационное обеспечение информационной безопасности : [учебник для вузов по специальностям "Организация и технология защиты информации" и "Комплексная защита объектов информации" направления подготовки "Информационная безопасность" ] / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М., 2008. - 188, [1] с.

**2.** Гончаренко Л. П. Управление безопасностью : учебное пособие / Л. П. Гончаренко, Е. С. Куценко ; Рос. экон. акад. им. Г. В. Плеханова. - Москва, 2010. - 272 с. : ил., табл.

**3.** Грушо А. А. Теоретические основы компьютерной безопасности : [учебное пособие по специальностям 090100 "Информационная безопасность"] / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М., 2009. - 267, [1] с. : ил.

**4.** Абденов А. Ж. Методика оценки риска для информационных систем на основе экспертных оценок : учебное пособие / А. Ж. Абденов, С. А. Белкин, Р. Н. Заркумова-Райхель ; Новосиб. гос. техн. ун-т. - Новосибирск, 2014. - 69, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000213163

*Интернет-ресурсы*

**1.** ЭБС НГТУ : http://elibrary.nstu.ru/

**2.** ЭБС «Издательство Лань» : https://e.lanbook.com/

**3.** ЭБС IPRbooks : http://www.iprbookshop.ru/

**4.** ЭБС "Znanium.com" : http://znanium.com/

**5.** :

## 8. Методическое и программное обеспечение

*8.1 Методическое обеспечение*

**1.** Курлаев С. А. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие / А. С. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000162258. - Загл. с экрана.

**2.** Дронова Г. А. Управление информационной безопасностью : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 23, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234012

*8.2 Специализированное программное обеспечение*

**1** Windows
**2** Office

## 9. Материально-техническое обеспечение

Презентационное оборудование

| № | Наименование | Назначение |
|---|---|---|
| 1 | Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления) | Для демонстрации основных положений курса |

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАНАВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

## УЧЕБНОЙ ДИСЦИПЛИНЫ

**Основы управления информационной безопасностью**

Образовательная программа: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по дисциплине Управление информационной безопасностью приведена в Таблице.

Таблица

| **Формируемые компетенции** | **Показатели сформированности компетенций (знания, умения, навыки)** | **Темы** | **Этапы оценки компетенций** | |
|---|---|---|---|---|
| | | | **Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)** | **Промежуточная аттестация (экзамен, зачет)** |
| ОК.2 способность использовать основы экономических знаний в различных сферах деятельности | у4. уметь оценивать управление предприятием с позиции внутреннего состояния и внешнего окружения | Информационные ресурсы организации. Типы ИР. Информационные активы и пассивы. Категорирование ИР. Классификация ИР по требованиям закона ФЗ-152 Модель угроз и модель нарушителя. Понятие. Образцы. Пример разработки Оценка рисков ИБ типовой организации. Разработка методов управления рисками типовой организации Процессы информационной безопасности, составляющие СУИБ организации (18 процессов). Разработка мероприятий и проведение процедур категорирования ИР и классификации ИСПДн типовой организации Система обеспечения ИБ как совокупность системы ИБ и системы управления ИБ. Цикл Демминга. Процессный подход к ИБ. Составляющие процесса. Оценка результативности процесса. Метрики. Уровни зрелости процессов | РГЗ, разделы 1.1-1.5. | Экзамен, Вопросы 1.1, 1.4, 1.6-1.10, 3.1-3.10 |
| ПК.13/ОУ способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | з1. знать основные методы управления информационной безопасностью | Аудит и мониторинг СУИБ. Понятие big-date. Применение agile технологий Процессы информационной безопасности, составляющие СУИБ организации (18 процессов). Процессы информационных технологий (37 процессов). Общие понятия. Связь с процессами ИБ. ИТ-контроли Разработка и внедрение СУИБ на основе процессов ИБ. Технические системы защиты информации. Классификация. Применение технических систем в разрезе процессного понимания СУИБ организации. Контроль использования технических систем | РГЗ, разделы 1.1-1.5. | Экзамен, Вопросы 1.2, 1.3, 1.5, 2.1-2.10 |
| ПК.6/Э способность принимать участие в организации и проведении | у1. уметь разрабатывать предложения по совершенствованию | Аудит и мониторинг СУИБ. Понятие big-date. Применение agile технологий Модель угроз и модель нарушителя. | РГЗ, разделы 1.1-1.5. | Экзамен, Вопросы 1.1-1.10, 2.1-2.10, 3.1-3.10 |

| | | | | |
|---|---|---|---|---|
| контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации | системы управления информационной безопасностью информационных систем | Понятие. Образцы. Пример разработки Процесс Управление рисками ИБ. Определение уязвимостей информационных ресурсов, вероятности реализации угроз и возможных финансовых потерь. Понятие риска ИБ. Методы управления рисками ИБ Процессы информационной безопасности, составляющие СУИБ организации (18 процессов). Процессы информационной безопасности, составляющие СУИБ организации (18 процессов). Порядок внедрения в деятельность организации Процессы информационных технологий (37 процессов). Общие понятия. Связь с процессами ИБ. ИТ-контроли | | |

**2. Методика оценки этапов формирования компетенций в рамках дисциплины.**

Промежуточная аттестация по дисциплине проводится в 7 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ОК.2, ПК.13/ОУ, ПК.6/Э Экзамен проводится по форме, приведенной в соответствующем паспорте.

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 7 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнениюРГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОК.2, ПК.13/ОУ, ПК.6/Э, за которые отвечает дисциплина, на разных уровнях.

**Общая характеристика уровней освоения компетенций.**

**Ниже порогового.** Теоретическое содержание курса освоено частично, пробелы носят существенный характер, уровень выполнения работы не отвечает большинству основных требований, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, предусмотренное программой обучения учебное задание не выполнено.

**Пороговый**. Теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, уровень выполнения работы отвечает большинству основных требований, необходимые практические навыки работы с освоенным материалом в основном сформированы.

**Базовый.** Теоретическое содержание курса освоено полностью, без пробелов, уровень выполнения работы отвечает всем основным требованиям, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

**Продвинутый.** Теоретическое содержание курса освоено полностью, без пробелов, уровень выполнения работы отвечает всем требованиям, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

# Паспорт экзамена

по дисциплине «Основы управления информационной безопасностью», 7 семестр

1. **Методика оценки**

Экзамен проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов __1__, второй вопрос из диапазона вопросов __2__, третий вопрос выбирается из диапазона вопросов __3__ (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня вопросов (п. 4).

# Форма экзаменационного билета

НОВОСИБИРСКИЙГОСУДАРСТВЕННЫЙТЕХНИЧЕСКИЙУНИВЕРСИТЕТ
Факультет АВТФ

**Билет №_____**
к экзамену по дисциплине «Основы управления информационной безопасностью»

1. Вопрос 1.
2. Вопрос 2.
3. Вопрос 3.

Утверждаю: зав. кафедрой ____должность, ФИО
(подпись)
(дата)

2. **Критерии оценки**

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы показывает слабые знания основных понятий ИБ, не понимает их взаимосвязь.
  Оценка составляет *_0_ баллов.*
- Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы показывает знание основных понятий ИБ, способен показать их взаимовлияние и зависимости, но не показывает понимания процессности в построении ИБ, роли СИБ и СУИБ в системе защиты информации.
  Оценка составляет *__30__ баллов*
- Ответ на экзаменационный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы показывает знание основных понятий ИБ, может показать их взаимозависимость, имеет понимание процесса ИБ, СИБ и СУИБ.
  Оценка составляет *__50__ баллов.*

- Ответ на экзаменационный билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы показывает знание основных понятий ИБ, может показать их взаимозависимость, имеет понимание процесса ИБ, системы ИБ и системы управления ИБ, организационной и технической составляющих ИБ, способен обосновать применение организационных мер и технических средств в процессах ИБ.
  Оценка составляет _70_ *баллов.*

**3. Шкала оценки**

В общей оценке по дисциплинеэкзаменационные баллыучитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

**4. Вопросы к экзамену по дисциплине «Основы управления информационной безопасностью»**

Диапазон 1.

1. Основные понятия ИБ и их взаимосвязь (на основе Common Criteria)
2. Роль и задачи СИБ, СУИБ
3. Процесс. Понятия и составляющие процесса
4. Информационные ресурсы. Типы ИР. Информационные активы
5. Идентификация и аутентификация
6. Модель угроз
7. Модель нарушителя
8. Процессный подход. Цикл Деминга
9. Понятие жизненного цикла. ЖЦ систем, проектов, услуг
10. Источники требований к ИБ

Диапазон 2.

1. Процесс ИБ. Управление рисками
2. Процесс ИБ. Контроль логического доступа
3. Процесс ИБ. Контроль соблюдения требований ИБ персоналом
4. Процесс ИБ. Осведомленность и информирование
5. Процесс ИБ. Физическая безопасность и защита от воздействия окружающей среды
6. Процесс ИБ. Управление инцидентами
7. Процесс ИБ. Защита систем и связи
8. Процесс ИБ. Системная и информационная целостность
9. Процесс ИБ. Управление конфигурацией
10. Процесс ИБ. Управление непрерывностью

Диапазон 3.

1. Описать этап Act цикла PDCA
2. Описать этап Do цикла PDCA
3. Описать этап Check цикла PDCA
4. Описать этап Plan цикла PDCA
5. Свойства информации - соответствие и подотчетность
6. Свойства информации - неотказуемость и аутентичность
7. Свойства информации - целостность и доступность
8. Свойства информации - полезность и эффективность
9. Свойства информации - конфиденциальность и надежность
10. Владелец информации и заказчик услуг ИБ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

# Паспорт
# расчетно-графического задания (работы)

по дисциплине «Основы уравления информационной безопасностью», 7 семестр

## 1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны разработать документ (политику информационной безопасности первого уровня), содержащий концептуальные положения системы управления информационной безопасности организации.

При выполнении расчетно-графического задания (работы) студенты должны провести анализ действующих международных и отечественных стандартов в области информационной безопасности, требований законодательства РФ и государственных регуляторов в области информационных технологий и защиты информации, отраслевых требований (применительно к предоставленной преподавателем организации), разработать концепцию информационной безопасности организации.

Обязательные структурные части РГЗ.

1. Политика (концепция) информационной безопасности организации.
2. Перечень использованных законодательных, нормативных документов, стандартов по информационной безопасности.

Оцениваемые позиции:

1. Документированная политика (концепция) ИБ.
2. Перечень используемых законодательных актов.
3. Перечень используемых международных и отечественных стандартов по ИБ.
4. Перечень используемых нормативных документов регуляторов.
5. Перечень используемых отраслевых требований

## 2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), не использованы требования законодательства, регуляторов, недостаточна степень использования стандартов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: законодательные требования и требования регуляторов, стандартов использованы в недостаточном объеме, отраслевые требования не использованы. Оценка составляет __10__ баллов.
- Работа считается выполненной **на базовом** уровне, если законодательные требования и требования стандартов использованы в полном объеме, требования регуляторов и отраслевые требования использованы частично. Оценка составляет __20__ баллов.
- Работа считается выполненной **на продвинутом** уровне, если требования законодательства, регуляторов, стандартов использованы в полном объеме, отраслевые требования использованы частично. Оценка составляет __30__ баллов.

## 3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ(Р) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Примерный перечень тем РГЗ(Р)**

На основе действующих в сфере информационной безопасности требований законодательства РФ, регуляторов, международных и отечественных стандартов, соответствующей отрасли разработать и задокументировать в текстовом редакторе "Концепцию информационной безопасности организации", определяющую стратегические направления защиты информации для одной из нижеприведенных компаний.

Вариант I. Крупное авиастроительное предприятие.

Вариант II. Фармацевтическое предприятие среднего уровня.

Вариант III. Государственная организация.

Вариант IV. Небольшое частное предприятие.