МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Институт компьютерных наук и технологий

Авторы-составители: **Лобков Армандо Львович**
Мустакимова Яна Романовна
Черников Арсений Викторович

Рабочая программа дисциплины

РОССИЙСКИЕ И МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Код УМК 69526

Утверждено
Протокол №6
от «06» мая 2022 г.

Пермь, 2022

1. Наименование дисциплины

Российские и международные стандарты защиты информации

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.01** Компьютерная безопасность

специализация Разработка защищенного программного обеспечения

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Российские и международные стандарты защиты информации** у обучающегося должны быть сформированы следующие компетенции:

10.05.01 Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

ПК.3 Способен принимать участие в разработке программных (программно-технических) средств защиты информации

Индикаторы

ПК.3.1 Ориентируется в методах разработки программных (программно-технических) средств защиты информации

ПК.3.2 Применяет на практике методы разработки программных (программно-технических) средств защиты информации

ОПСК.1 Способен проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

Индикаторы

ОПСК.1.1 Ориентируется в требованиях нормативных документов по разработке программного кода

ОПСК.1.2 Выполняет тестирование программного кода

ОПСК.1.3 Применяет на практике методы и средства анализа программного кода

ОПСК.1.4 Осуществляет поиск потенциальных уязвимостей и недокументированных возможностей программного кода

4. Объем и содержание дисциплины

Специальность	10.05.01 Компьютерная безопасность (специализация: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	14
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	56
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	28
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (2)
Формы промежуточной аттестации	Экзамен (14 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Российские и международные стандарты защиты информации

Раздел 1 Американские и европейские стандарты защиты информации ограниченного доступа

Европейские стандарты по обеспечению информационной безопасности.
- гармонизированные критерии Европейских стран;
- стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" .

Британский стандарт BS 7799 по обеспечению информационной безопасности.
- обзор стандарта BS 7799;
- регуляторы безопасности и реализуемые ими цели;
- четырехфазная модель процесса управления информационной безопасностью.

Стандарты Германии, США по обеспечению информационной безопасности.
- немецкий стандарт BSI;
- американские "Федеральные критерии безопасности информационных технологий".

Национальный стандарт Канады по обеспечению информационной безопасности.
- канадские "Критерии безопасности компьютерных систем".

Международный стандарт COBIT по обеспечению информационной безопасности.
- назначение стандарта COBIT;
- принципы управления информационными технологиями на базе стандарта COBIT.

Раздел 2 Серия международных стандартов ISO 27000

Вопросы безопасности.
- безопасность связанная с персоналом;
- физическая безопасность и защита от воздействия окружающей среды.

Менеджмент коммуникаций.
- эксплуатационные процедуры и обязанности;
- менеджмент оказания услуг третьей стороной, планирование и приемка систем;
- защита от вредоносных и мобильных программ, резервирование.

Безопасность информационных сетей и обмен информацией.
- менеджмент безопасности сети, обращение с носителями информации;
- обмен информацией.

Управление доступом.
- требования бизнеса по управлению доступом;
- управление доступом к сетям.

Приобретение, разработка и эксплуатация информационных систем.
- требования к безопасности информационных систем, корректная обработка в прикладных программах;
- криптографические меры и средства контроля и управления;
- безопасность системных файлов.

Раздел 3 Российские стандарты в области защиты информации ограниченного доступа

Стандарты по обеспечению информационной безопасности в Российской Федерации.

- стандарты и руководящие документы в области защиты информации ограниченного доступа.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Торокин А. А. Инженерно-техническая защита информации:учебное пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности/А. А. Торокин.-Москва:Гелиос АРВ,2005, ISBN 5-85438-140-0.-960.-Библиогр.: с. 934-949

Дополнительная:

1. Северин В. А. Правовая защита информации в коммерческих организациях:учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Юриспруденция" направления "Юриспруденция" : учебное пособие для студентов высших учебных заведений, обучающихся по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информатизации" направления подготовки "Информационная безопасность"/В. А. Северин ; ред. Б. И. Пугинский.-Москва:Академия,2009, ISBN 978-5-7695-5563-3.-2191.-Библиогр.: с. 216-218

2. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности:учебное пособие для студентов, обучающихся по программам высшего образования укрупненной группы специальностей и направлений подготовки 10.00.00 "Информационная безопасность"/Ю. А. Родичев.-Санкт-Петербург:Питер,2018, ISBN 978-5-4461-0861-9.-256.-Библиогр.: с. 240-244

3. Логунов А. Б. Региональная и национальная безопасность:учебное пособие/А.Б. Логунов.-Москва:Вузовский учебник,2011 [т.е. 2010], ISBN 978-5-9558-0161-2.-4471.-Библиогр.: с. 442-445 и в подстроч. примеч.

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

http://www.psu.ru/ elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
http://window.edu.ru/ Единое окно доступа к образовательным ресурсам

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Российские и международные стандарты защиты информации** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине "Российские и международные стандарты защиты информации" предполагает использование следующего программного обеспечения и информационных справочных систем:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета.
Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов "Adobe Acrobat Reader DC";
- офисный пакет приложений "LibreOffice";
- MS Word; MS Excel; Multisim; MathCAD.
При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (student.psu.ru).

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения практических занятий - аудитория, аудитория оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для групповых (индивидуальных) консультаций - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения текущего контроля - аудитория, оснащенная меловой (и) или маркерной доской.
Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью

подключения к сети «Интернет» с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения Научной библиотеки ПГНИУ.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Российские и международные стандарты защиты информации

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ОПСК.1

Способен проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПСК.1.1 Ориентируется в требованиях нормативных документов по разработке программного кода	Знать основные требования нормативных документов по разработке защищенного программного кода. Уметь применять требования нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Владеть навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода.	**Неудовлетворител** Не знает основные требования нормативных документов по разработке защищенного программного кода. Не умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Не владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода. **Удовлетворительн** Знает не все основные требования нормативных документов по разработке защищенного программного кода. Плохо умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Не владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода. **Хорошо** Знает все основные требования нормативных документов по разработке защищенного программного кода. Хорошо умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Не в полной мере владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Знает все основные требования нормативных документов по разработке защищенного программного кода. Хорошо умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. В полной мере владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода.
ОПСК.1.2 Выполняет тестирование программного кода	Знать основные методы тестирования программного кода. Уметь применять методы тестирования программного кода. Владеть навыками тестирования программного кода при решении профессиональных задач.	**Неудовлетворител** Не знает основные методы тестирования программного кода. Не умеет применять методы тестирования программного кода. Не владеет навыками тестирования программного кода при решении профессиональных задач **Удовлетворительн** Знает основные методы тестирования программного кода. Не умеет применять методы тестирования программного кода. Не владеет навыками тестирования программного кода при решении профессиональных задач **Хорошо** Знает основные методы тестирования программного кода. Умеет применять методы тестирования программного кода. Владеет не в полной мере навыками тестирования программного кода при решении профессиональных задач. **Отлично** Знает основные методы тестирования программного кода. Умеет применять методы тестирования программного кода. Владеет в полной мере навыками тестирования программного кода при решении профессиональных задач.
ОПСК.1.3	Знать основные методы и	**Неудовлетворител**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
Применяет на практике методы и средства анализа программного кода	средства анализа программного кода. Уметь применять основные методы и средства анализа программного кода. Владеть навыками применения методов и средств анализа программного кода при решении профессиональных задач.	**Неудовлетворител** Не знает основные методы и средства анализа программного кода. Не умеет применять основные методы и средства анализа программного кода. Не владеет навыками применения методов и средств анализа программного кода при решении профессиональных задач. **Удовлетворительн** Знает основные методы и средства анализа программного кода. Не умеет применять основные методы и средства анализа программного кода. Не владеет навыками применения методов и средств анализа программного кода при решении профессиональных задач. **Хорошо** Знает основные методы и средства анализа программного кода. Умеет применять основные методы и средства анализа программного кода. Владеет не в полной мере навыками применения методов и средств анализа программного кода при решении профессиональных задач. **Отлично** Знает основные методы и средства анализа программного кода. Умеет применять основные методы и средства анализа программного кода. Владеет в полной мере навыками применения методов и средств анализа программного кода при решении профессиональных задач
ОПСК.1.4 Осуществляет поиск потенциальных уязвимостей и недокументированных возможностей программного кода	Знать основные уязвимости и недокументированные возможности программного кода. Уметь проверять программный код на наличие потенциальных уязвимостей и недокументированных возможностей. Владеет методами поиска потенциальных уязвимостей и	**Неудовлетворител** Не знает основные уязвимости и недокументированные возможности программного кода. Не умеет проверять программный код на наличие потенциальных уязвимостей и недокументированных возможностей. Не владеет методами поиска потенциальных уязвимостей и недокументированных возможностей программного кода. **Удовлетворительн**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	недокументированных возможностей программного кода.	**Удовлетворительн** Знает основные уязвимости и недокументированные возможности программного кода. Частично умеет проверять программный код на наличие потенциальных уязвимостей и недокументированных возможностей. Не владеет методами поиска потенциальных уязвимостей и недокументированных возможностей программного кода. **Хорошо** Знает основные уязвимости и недокументированные возможности программного кода. Полностью умеет проверять программный код на наличие потенциальных уязвимостей и недокументированных возможностей. Владеет не в полной мере методами поиска потенциальных уязвимостей и недокументированных возможностей программного кода. **Отлично** Знает основные уязвимости и недокументированные возможности программного кода. Полностью умеет проверять программный код на наличие потенциальных уязвимостей и недокументированных возможностей. Владеет в полной мере методами поиска потенциальных уязвимостей и недокументированных возможностей программного кода.

ПК.3

Способен принимать участие в разработке программных (программно-технических) средств защиты информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.3.1 Ориентируется в методах разработки программных (программно-технических) средств защиты информации	Знать методы разработки программных (программно-технических) средств защиты информации. Уметь находить информацию по методам разработки программных (программно-	**Неудовлетворител** Не знает методы разработки программных (программно-технических) средств защиты информации. Не умеет находить информацию по методам разработки программных (программно-технических) средств защиты информации.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	технических) средств защиты информации. Владеть навыками поиска, анализа и обобщения информации о методах разработки программных (программно-технических) средств защиты информации.	**Неудовлетворител** Не владеет навыками поиска, анализа и обобщения информации о методах разработки программных (программно-технических) средств защиты информации. **Удовлетворительн** Знает основные методы разработки программных (программно-технических) средств защиты информации. Частично умеет находить информацию по методам разработки программных (программно-технических) средств защиты информации. Не владеет навыками поиска, анализа и обобщения информации о методах разработки программных (программно-технических) средств защиты информации. **Хорошо** Знает все методы разработки программных (программно-технических) средств защиты информации. Умеет в полной мере находить информацию по методам разработки программных (программно-технических) средств защиты информации. Не владеет в полной мере навыками поиска, анализа и обобщения информации о методах разработки программных (программно-технических) средств защиты информации. **Отлично** Знает все методы разработки программных (программно-технических) средств защиты информации. Умеет в полной мере находить информацию по методам разработки программных (программно-технических) средств защиты информации. Владеет в полной мере навыками поиска, анализа и обобщения информации о методах разработки программных (программно-технических) средств защиты информации.
ПК.3.2 Применяет на практике методы разработки программных	Знать методы разработки программных (программно-технических) средств защиты информации.	**Неудовлетворител** Не знает методы разработки программных (программно-технических) средств защиты информации.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
(программно-технических) средств защиты информации	Уметь применять на практике методы разработки программных (программно-технических) средств защиты информации. Владеть навыками разработки программных (программно-технических) средств защиты информации в соответствии с профессиональными задачами.	**Неудовлетворител** Не умеет применять на практике методы разработки программных (программно-технических) средств защиты информации. Не владеет навыками разработки программных (программно-технических) средств защиты информации в соответствии с профессиональными задачами. **Удовлетворительн** Знает основные методы разработки программных (программно-технических) средств защиты информации. Умеет с ошибками применять на практике методы разработки программных (программно-технических) средств защиты информации. Не владеет навыками разработки программных (программно-технических) средств защиты информации в соответствии с профессиональными задачами. **Хорошо** Знает основные методы разработки программных (программно-технических) средств защиты информации. Умеет без ошибок применять на практике методы разработки программных (программно-технических) средств защиты информации. Не владеет в полной мере навыками разработки программных (программно-технических) средств защиты информации в соответствии с профессиональными задачами. **Отлично** Знает основные методы разработки программных (программно-технических) средств защиты информации. Умеет без ошибок применять на практике методы разработки программных (программно-технических) средств защиты информации. Владеет в полной мере навыками разработки программных (программно-технических) средств защиты информации в соответствии с профессиональными задачами.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС КМБ

Вид мероприятия промежуточной аттестации : Экзамен
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 41 до 60
«неудовлетворительно» / «незачтено» менее 41 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.3.2 Применяет на практике методы разработки программных (программно-технических) средств защиты информации **ПК.3.1** Ориентируется в методах разработки программных (программно-технических) средств защиты информации	Европейские стандарты по обеспечению информационной безопасности. **Письменное контрольное мероприятие**	Знание Европейских стандартов
ОПСК.1.2 Выполняет тестирование программного кода **ОПСК.1.3** Применяет на практике методы и средства анализа программного кода **ОПСК.1.4** Осуществляет поиск потенциальных уязвимостей и недокументированных возможностей программного кода **ОПСК.1.1** Ориентируется в требованиях нормативных документов по разработке программного кода	Вопросы безопасности. **Итоговое контрольное мероприятие**	Знание международных стандартов

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПСК.1.2 Выполняет тестирование программного кода **ОПСК.1.1** Ориентируется в требованиях нормативных документов по разработке программного кода **ОПСК.1.4** Осуществляет поиск потенциальных уязвимостей и недокументированных возможностей программного кода **ОПСК.1.3** Применяет на практике методы и средства анализа программного кода **ПК.3.1** Ориентируется в методах разработки программных (программно-технических) средств защиты информации **ПК.3.2** Применяет на практике методы разработки программных (программно-технических) средств защиты информации	Стандарты по обеспечению информационной безопасности в Российской Федерации. **Письменное контрольное мероприятие**	Знание Российских стандартов

Спецификация мероприятий текущего контроля

Европейские стандарты по обеспечению информационной безопасности.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12.3**

Показатели оценивания	Баллы
Знание стандарта BSI	8
Знание стандарта ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"	8
Знание гармонизированных критерий Европейских стран	7
Знание стандарта BS 7799	7

Вопросы безопасности.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12.3**

Показатели оценивания	Баллы
Знание серии международных стандартов ISO 27000	15
Знание принципов управления информационными технологиями на базе стандарта COBIT	8
Знание назначения международного стандарта COBIT	7

Стандарты по обеспечению информационной безопасности в Российской Федерации.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **16.4**

Показатели оценивания	Баллы
Знание процедур по защите информации в соответствии со стандартом РФ ГОСТ Р ИСО/МЭК 27002-2012	20
Знание основных положений национального стандарта РФ ГОСТ Р ИСО/МЭК 27002-2012. «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»	20