

**МИНОБРНАУКИ РОССИИ**

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

**Кафедра информационной безопасности и систем связи**

Авторы-составители: **Пенский Олег Геннадьевич  
Карпов Михаил Юрьевич**

Рабочая программа дисциплины  
**ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ**  
Код УМК 91350

Утверждено  
Протокол №1  
от «06» мая 2022 г.

Пермь, 2022

## **1. Наименование дисциплины**

Основы кибербезопасности

## **2. Место дисциплины в структуре образовательной программы**

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

Направление подготовки: **44.03.05** Педагогическое образование (с двумя профилями подготовки)  
направленность Биология и Физическая культура

### **3. Планируемые результаты обучения по дисциплине**

В результате освоения дисциплины **Основы кибербезопасности** у обучающегося должны быть сформированы следующие компетенции:

**44.03.05** Педагогическое образование (с двумя профилями подготовки) (направленность : Биология и Физическая культура)

**ОПК.10** Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности

#### **Индикаторы**

**ОПК.10.1** Демонстрирует базовые знания в области информационно-коммуникационных технологий

**ОПК.10.2** Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности

#### 4. Объем и содержание дисциплины

<b>Направление подготовки</b>	44.03.05 Педагогическое образование (с двумя профилями подготовки) (направленность: Биология и Физическая культура)
<b>форма обучения</b>	очная
<b>№№ триместров, выделенных для изучения дисциплины</b>	13
<b>Объем дисциплины (з.е.)</b>	3
<b>Объем дисциплины (ак.час.)</b>	108
<b>Контактная работа с преподавателем (ак.час.), в том числе:</b>	42
<b>Проведение лекционных занятий</b>	14
<b>Проведение практических занятий, семинаров</b>	28
<b>Самостоятельная работа (ак.час.)</b>	66
<b>Формы текущего контроля</b>	Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (3)
<b>Формы промежуточной аттестации</b>	Зачет (13 триместр)

## 5. Аннотированное описание содержания разделов и тем дисциплины

### **Кибербезопасность в системе национальной безопасности РФ**

Студенты должны усвоить то, что компьютерная безопасность является частью информационной безопасности государства, должны понять общие принципы построения СЗИ и формализацию в подходе построения СЗИ, студенты должны научиться применять при построении оценки эффективности СЗИ правила четкой и нечеткой математики, уметь использовать методы экспертных оценок при создании СЗИ, должны создать СЗИ ПК и оценить ее эффективность с помощью всех изученных методов и применении метода экспертного оценивания DELPHI, должны понять общие принципы работы хакеров в сети Интернет и уметь работать в сети с наибольшей вероятностью предохранения от утечек информации, должны усвоить принципы организации работы СЗИ в банковских структурах и узнать современные основные угрозы ИС, должны узнать об основных типах сетей и классификации СЗИ этих сетей. При рассмотрении данной темы необходимо дать характеристики следующим неопределенностям, влияющим на адекватность работы СЗИ:

- Неясное представление целей СЗИ;
- Неясное представление угроз и ущерба от наступающих угроз;
- Отсутствие точных методов оценки эффективности СЗИ.

### **Информационная война, методы и средства её ведения**

При рассмотрении данной темы необходимо сформировать у студентов твердые навыки по использованию матрицы знаний при создании СЗИ. Студент должен разработать программу, позволяющую заполнять элементы матрицы знаний в ходе создания СЗИ. На лекции преподаватель рассказывает о структуре матрицы знаний и контроле создания СЗИ на основе этой матрицы знаний. При рассмотрении данной темы необходимо сформировать у студентов практические навыки построения матрицы знаний, как основном механизме планирования создания СЗИ. Студентам в качестве практического задания предлагается разработать компьютерную программу, формирующую матрицу знаний для ПК. Текущим контролем усвоения материалов темы является защита плана построения СЗИ ПК с помощью матрицы знаний перед аудиторией.

### **Критерии защищенности компьютерных систем**

Студент должен понять общие свойства большинства математических моделей и методов оценки эффективности СЗИ. Он должен знать то, все методы носят оценочный и приближенный характер, часто использующий экспертное оценивание и, как нечеткие, так и четкие характеристики. Студенты должны понять, что, исходя из этого, матмодели СЗИ делятся на три типа: основанные на теории четкой математики, нечеткой математики и использующие смешанные основы.

Студент, основываясь на знаниях теории вероятностей и понятиях теории нечетких множеств, должен освоить методы построения функции ущерба СЗИ и вычислять численные значения этой функции для конкретных СЗИ. Студент должны уметь применять расчеты для определения наиболее эффективной СЗИ из заданных СЗИ.

### **Защита информации, обрабатываемой в автоматизированных системах**

Студент должен получить твердые навыки при создании СЗИ с оценкой их эффективности с помощью математических моделей. Преподаватель на лекции рассказывает пример создания простейшей СЗИ ПК с использованием математических моделей. Он обращает особое внимание на оценку экономических затрат создания и функционирования СЗИ, как основном факторе, определяющим выбор при внедрении СЗИ.

### **Закон РФ о государственной тайне**

Рассматривается закон РФ о гостайне. В частности, изучаются вопросы, касающиеся засекречивания и рассекречивания информации, общих принципов составления перечня закрытых тем, служебных

полномочий структур по засекречиванию информации, возможности открытых публикаций и патентов.

### **Безопасность сети интернет**

Интернет.

Студент должен изучить следующие вопросы:

1. Интернет в структуре информационно-аналитического обеспечения.
2. Основные протоколы Интернет и их использование злоумышленниками.
3. Аутентификация в Интернет.
4. Легкость наблюдения за передаваемыми данными.
5. Потенциальные проблемы с электронной почтой.

### **Компьютерные вирусы и антивирусные продукты**

Понятие компьютерного вируса. Признаки заражения компьютера. История возникновения вирусов.

Классификации компьютерных вирусов. Пути проникновения вирусов на компьютер. Методы защиты от компьютерных вирусов. Антивирусные программы

## **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 аудиторские 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. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. <https://www.urait.ru/bcode/422772>
2. Горев, А. И. Обработка и защита информации в компьютерных системах : учебно-практическое пособие / А. И. Горев, А. А. Симаков. — Омск : Омская академия МВД России, 2016. — 88 с. — ISBN 978-5-88651-642-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/72856.html>

### Дополнительная:

1. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/33430>
2. Савицкий, А. Г. Национальная безопасность. Россия в мире : учебник для студентов вузов / А. Г. Савицкий. — Москва : ЮНИТИ-ДАНА, 2017. — 463 с. — ISBN 978-5-238-02307-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/81509.html>
3. Ермаков, Д. Г. Применение антивирусных программ для обеспечения информационной безопасности / Д. Г. Ермаков, А. В. Присяжный. — Екатеринбург : Уральский федеральный университет, ЭБС АСВ, 2013. — 64 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. <http://www.iprbookshop.ru/66577.html>
4. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 с. — ISBN 978-5-4497-1653-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. <https://www.iprbookshop.ru/120489>

## **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 **Основы кибербезопасности** 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 «AdobeAcrobatReader DC»;
- офисный пакет приложений «LibreOffice», AltLinux

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 - компьютерный класс. Состав оборудования определен в Паспорте компьютерного класса.

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  
Основы кибербезопасности**

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

**ОПК.10**

**Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<p><b>ОПК.10.1</b> Демонстрирует базовые знания в области информационно-коммуникационных технологий</p>	<p>Знать основы информационно-коммуникационных технологий, основные требования информационной безопасности при работе с информационно-коммуникационными технологиями. Уметь применять информационно-коммуникационные технологии при решении профессиональных задач. Владеть навыками работы с информационно-коммуникационными технологиями.</p>	<p align="center"><b>Неудовлетворител</b></p> <p>Знает менее 50% основных понятий в области информационно-коммуникационных технологий. Не умеет использовать информационно-коммуникационные технологии с учетом требований по информационной безопасности. Не владеет навыками работы с информационно-коммуникационными технологиями.</p> <p align="center"><b>Удовлетворительн</b></p> <p>Знает не менее 50% основных понятий в области информационно-коммуникационных технологий. Умеет использовать информационно-коммуникационные технологии с учетом требований по информационной безопасности. Не владеет навыками работы с информационно-коммуникационными технологиями.</p> <p align="center"><b>Хорошо</b></p> <p>Знает не менее 70% основных понятий в области информационно-коммуникационных технологий. Умеет использовать информационно-коммуникационные технологии с учетом требований по информационной безопасности. Не в полной мере владеет навыками работы с информационно-коммуникационными технологиями.</p> <p align="center"><b>Отлично</b></p> <p>Знает основные понятия в области</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;"><b>Отлично</b></p> <p>информационно-коммуникационных технологий. Умеет использовать информационно-коммуникационные технологии с учетом требований по информационной безопасности. Владеет навыками работы с информационно-коммуникационными технологиями.</p>
<p><b>ОПК.10.2</b> Ориентировавшись на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности</p>	<p>Знать основные требования по информационной безопасности. Уметь использовать информационно-коммуникационные технологии в своей профессиональной деятельности с учетом требований информационной безопасности. Владеть методиками выбора информационно-коммуникационных технологий с учетом требований информационной безопасности.</p>	<p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не знает основные требования по информационной безопасности. Не умеет использовать информационно-коммуникационные технологии в своей профессиональной деятельности с учетом требований информационной безопасности. Не владеет методиками выбора информационно-коммуникационных технологий с учетом требований информационной безопасности.</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Знает основные требования по информационной безопасности. Не умеет использовать информационно-коммуникационные технологии в своей профессиональной деятельности с учетом требований информационной безопасности. Не владеет методиками выбора информационно-коммуникационных технологий с учетом требований информационной безопасности.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Знает основные требования по информационной безопасности. Умеет использовать информационно-коммуникационные технологии в своей профессиональной деятельности с учетом требований информационной безопасности. Не владеет методиками выбора информационно-коммуникационных технологий с учетом требований информационной безопасности.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Знает основные требования по информационной безопасности.</p>

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
		<p style="text-align: center;"><b>Отлично</b></p> <p>Умеет использовать информационно-коммуникационные технологии в своей профессиональной деятельности с учетом требований информационной безопасности. Владеет методиками выбора информационно-коммуникационных технологий с учетом требований информационной безопасности.</p>

## Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

**Вид мероприятия промежуточной аттестации :** Зачет

**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
<b>ОПК.10.1</b> Демонстрирует базовые знания в области информационно-коммуникационных технологий	Кибербезопасность в системе национальной безопасности РФ <b>Письменное контрольное мероприятие</b>	Письменная контрольная работа (тест), включающая в себя основные термины по проблематике кибербезопасности; показатели качества и критерии оценки систем и отдельных методов и средств обеспечения кибербезопасности; требования нормативных документов регламентирующие технические и программные меры обеспечения кибербезопасности; варианты решения задачи обеспечения кибербезопасности компьютерных систем
<b>ОПК.10.1</b> Демонстрирует базовые знания в области информационно-коммуникационных технологий	Защита информации, обрабатываемой в автоматизированных системах <b>Письменное контрольное мероприятие</b>	Письменная контрольная работа (тест), включающая в себя понятие кибербезопасности в системе национальной безопасности страны; угрозы кибербезопасности государства; содержание информационной войны, методы и средства ее ведения; современные подходы к построению систем кибербезопасности; общие принципы работы хакеров в сети Интернет, аутентификация в Интернет, проблемы с передачей данных по электронной почте.

<b>Компетенция (индикатор)</b>	<b>Мероприятие текущего контроля</b>	<b>Контролируемые элементы результатов обучения</b>
<p><b>ОПК.10.2</b> Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности</p>	<p>Закон РФ о государственной тайне <b>Письменное контрольное мероприятие</b></p>	<p>Письменная контрольная работа (тест), включающая в себя вопросы о современных подходах к построению систем кибербезопасности; о компьютерной системе как объекту информационного воздействия, о критериях оценки ее защищенности и методах обеспечения ее кибербезопасности; международное законодательство по кибербезопасности; определение мер и мероприятий по защите программными средствами, обоснование лучших вариантов защиты особенности обеспечения кибербезопасности компьютерных систем при обработке информации, составляющей государственную тайну; вторжения в компьютерную систему методами удаленного доступа, вторжения в систему при наличии локального доступа; вторжения в мобильные устройства, новые тенденции; антивирусные программы, их достоинства и недостатки, особенности применения.</p>
<p><b>ОПК.10.2</b> Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности <b>ОПК.10.1</b> Демонстрирует базовые знания в области информационно-коммуникационных технологий</p>	<p>Компьютерные вирусы и антивирусные продукты <b>Итоговое контрольное мероприятие</b></p>	<p>Письменная контрольная работа (тест), включающая в себя набор понятий и терминов дисциплины, нормативных актов.</p>

### Спецификация мероприятий текущего контроля

**Кибербезопасность в системе национальной безопасности РФ**

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **8.2**

<b>Показатели оценивания</b>	<b>Баллы</b>
Знать методы нарушения конфиденциальности, целостности и доступности информации; причины, виды, каналы утечки и искажения информации	4
Знать угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России; внешние источники угроз, внутренние источники угроз	4
Знать методы воздействия на компьютерную систему	3
Знать основные понятия и определения из нормативных документов РФ по кибербезопасности	3
Знать основные составляющие национальных интересов Российской Федерации в информационной сфере	3
Знать общеметодологические принципы теории кибербезопасности. Роль кибербезопасности в обеспечении национальной безопасности государства	3

### **Защита информации, обрабатываемой в автоматизированных системах**

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **16.4**

<b>Показатели оценивания</b>	<b>Баллы</b>
Способность выполнить учебно – теоретическую задачу по созданию концептуальной модели объекта защиты и обоснованию выбранных средств и методов защиты.	8
Знать методы и средства компьютерной разведки, технические каналы утечки информации при эксплуатации АС	8
Знать алгоритмы оценки качества систем защиты	6
Уметь по заданным параметрам обосновать критерии защиты защищаемого объекта по требованиям безопасности информации	6
Знать организационно-правовые, технические и криптографические методы обеспечения кибербезопасности; программно-аппаратные средства обеспечения кибербезопасности	6
Знать модели, стратегии и системы обеспечения кибербезопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	6

### **Закон РФ о государственной тайне**

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **8.2**

<b>Показатели оценивания</b>	<b>Баллы</b>
------------------------------	--------------

Знать методы вторжения злоумышленников в компьютерную систему методами удаленного доступа, вторжения в систему при наличии локального доступа, вторжения в мобильные устройства, новые тенденции.	7
Знать общие положения законодательства по защите государственной тайны, перечень сведений, подлежащих засекречиванию, порядок рассекречивания документов	5
Знать общие принципы работы хакеров в сети Интернет	5
Антивирусные программы, обоснование лучших вариантов защиты	3

### **Компьютерные вирусы и антивирусные продукты**

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **8.2**

<b>Показатели оценивания</b>	<b>Баллы</b>
Уметь решать учебно-теоретические и практические задачи по кибербезопасности	10
Знать основные понятия и нормативные документы по кибербезопасности	10