

**ГАОУ ВО «Дагестанский государственный университет  
народного хозяйства»**

*Утверждена решением  
Ученого совета ДГУНХ,  
протокол № 13  
от 06 июля 2020 г*

**Кафедра «Информационные технологии и информационная  
безопасность»**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗ-  
ОПАСНОСТЬЮ»**

**Направление подготовки**

**10.03.01 Информационная безопасность,**

**профиль «Безопасность автоматизированных систем»**

**Уровень высшего образования - бакалавриат**

**Форма обучения – очная**

**Махачкала – 2020**

**УДК 681.518(075.8)**

**ББК 32.81.73**

**Составитель** – Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внутренний рецензент** – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внешний рецензент** – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры "Математические методы в экономике" Дагестанского государственного университета.

**Представитель работодателя** - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

*Рабочая программа дисциплины «Основы управления информационной безопасностью» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г., № 1515, в соответствии с приказом Министерства образования и науки Российской Федерации от 5.04.2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»*

Рабочая программа по дисциплине «Основы управления информационной безопасностью» размещена на официальном сайте [www.dgunh.ru](http://www.dgunh.ru)

Гасанова З.А. Рабочая программа по дисциплине «Основы управления информационной безопасностью» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2020 г., 15 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 03 июля 2020 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 30 июня 2020 г., протокол № 12

## Содержание

|           |  |    |
|-----------|--|----|
| Раздел 1. | Перечень планируемых результатов обучения по дисциплине  | 4  |
| Раздел 2. | Место дисциплины в структуре образовательной программы   | 6  |
| Раздел 3. | Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся и форму промежуточной аттестации | 6  |
| Раздел 4. | Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий  | 8  |
| Раздел 5. | Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины   | 10 |
| Раздел 6. | Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины  | 12 |
| Раздел 7. | Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных  | 12 |
| Раздел 8. | Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине   | 13 |
| Раздел 9. | Образовательные технологии   | 14 |
|           | Лист актуализации рабочей программы дисциплины   | 15 |

## Раздел 1. Перечень планируемых результатов обучения по дисциплине

Целью дисциплины «Основы управления информационной безопасностью» является формирование у студентов компетенции обучающегося в области основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта.

Задачами дисциплины являются:

- Рассмотреть основы управления информационной безопасностью.
- Раскрыть принципы проектирования и реализации системы управления информационной безопасностью (ИБ) конкретного объекта
- Показать особенности сопровождения системы управления информационной безопасностью на предприятиях различных масштабов и отраслевой принадлежности.

### 1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «Основы управления информационной безопасностью» как часть планируемых результатов освоения образовательной программы

| код компетенции | формулировка компетенции   |
|-----------------|--|
| <b>ОПК</b>      | <b>ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ</b>  |
| <b>ОПК-7</b>    | Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты |
| <b>ПК</b>       | <b>ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ</b>  |
| <b>ПК-4</b>     | Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты  |
| <b>ПК-13</b>    | Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации   |

### 1.2 Планируемые результаты обучения по дисциплине

| код и формулировка компетенции  | компонентный состав компетенции  |   |   |
|---|--|---|---|
|   | знать  | уметь   | владеть                                     |
| <b>ОПК-7:</b> Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути | З1 - основные угрозы безопасности информации и модели нарушителя в информационных системах;<br>З2 - методики анализа | У1 - проводить классификацию критических информационных ресурсов;<br>У2 - анализировать | В3 - методами оценки информационных рисков. |

|   |   |  |   |
|---|---|--|---|
| их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты  | рисков;<br>ЗЗ - программные средства анализа и управления рисками.  | и оценивать информационные риски;<br>УЗ - разрабатывать модели угроз и нарушителей информационной безопасности информационных систем   |   |
| <b>ПК-4:</b> Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты          | З1 - принципы формирования политики информационной безопасности в информационных системах.  | У1 - разрабатывать частные политики информационной безопасности информационных систем.   | В1 – навыками разработки политики безопасности  |
| <b>ПК- 13:</b> Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | З1 - основные стандарты управления ИБ;<br>З2 - основные методы управления информационной безопасностью;<br>З3 - основы организации и методологии проведения аудита ИБ;<br>З4 - методы и инструментальные средства проведения активного аудита ИБ. | У1 - разрабатывать организационно-распорядительные документы системы менеджмента инцидентов информационной безопасности организации;<br>У2 - организовывать деятельность по обнаружению и реагированию на инциденты информационной безопасности в организациях, информационных системах;<br>УЗ - разрабатывать предложения по совершенствованию системы управления информационной безопасностью. | В1 - терминологией и процессным подходом построения систем управления ИБ;<br>В2 - методами организации и управления деятельностью служб защиты информации на предприятии;<br>В3 - Методами проведения аудита системы ИБ;<br>методами В4 - управления информационной безопасностью |

### 1.3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

| Код компетенции | Этапы формирования компетенций |         |         |         |         |         |         |
|-----------------|--------------------------------|---------|---------|---------|---------|---------|---------|
|                 | Тема 1.                        | Тема 2. | Тема 3. | Тема 4. | Тема 5. | Тема 6. | Тема 7. |
|                 |                                |         |         |         |         |         |         |

|              | Принципы, подходы и виды управления. Циклическая модель PDCA | Стратегии построения и внедрения СУИБ в организации | Назначение, структура и содержание Политики ИБ. Разработка политики безопасности | Управление рисками | Управление инцидентами ИБ | Аудит ИБ | Современные методы и средства анализа и управление рисками информационных систем компаний |
|--------------|--|---|--|--------------------|---------------------------|----------|---|
| <b>ОПК-7</b> |  |   |  | +                  |                           |          | +   |
| <b>ПК-4</b>  |  |   | +  | +                  |                           |          |   |
| <b>ПК-13</b> | +  | +   | +  |                    | +                         | +        |   |

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

Дисциплина Б1.Б.29 «Основы управления информационной безопасностью» относится к базовой части Блока 1 «Дисциплины» учебного плана направления подготовки «Информационная безопасность», профиля «Безопасность автоматизированных систем».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам «Основы информационной безопасности», «Основы управленческой деятельности», «Документоведение и документооборот».

Освоение данной дисциплины необходимо обучающемуся для изучения дисциплин «Комплексное обеспечение защиты информации объекта информатизации», «Оценка экономической эффективности системы защиты информации».

## **Раздел 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся, на самостоятельную работу обучающихся и форму промежуточной аттестации**

Объем дисциплины в зачетных единицах составляет 3 зачетные единицы.

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 32 часа, в том числе:

на занятия лекционного типа – **16** ч.

на занятия семинарского типа – **16** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **76** ч.

Форма промежуточной аттестации: зачет.

**Раздел 4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.**

| № п/п | Тема дисциплины  | Всего академических часов | В т.ч. занятия лекционного типа | В т.ч. занятия семинарского типа: |                      |  |             |                          | Самостоятельная работа | Форма текущего контроля успеваемости.  |
|-------|--|---------------------------|---------------------------------|-----------------------------------|----------------------|--|-------------|--------------------------|------------------------|--|
|       |  |                           |                                 | семинары                          | Практические занятия | Лабораторные занятия (лабораторные работы, лабораторный практикум) | Коллоквиумы | Иные аналогичные занятия |                        |  |
| 1.    | Тема 1. Принципы, подходы и виды управления. Циклическая модель PDCA | 12                        | 2                               | -                                 | 2                    | -  | -           | -                        | 8                      | Устный опрос<br>Тестирование<br>Подготовка реферата<br>Подготовка презентации<br>Решение кейса                       |
| 2.    | Тема 2. Стратегии построения и внедрения СУИБ в организации          | 12                        | 2                               | -                                 | 2                    | -  | -           | -                        | 8                      | Устный опрос<br>Подготовка реферата<br>Подготовка презентации<br>Письменная работа                                   |
| 3.    | Тема 3. Назначение структура и содержание Политики ИБ                | 14                        | 2                               | -                                 | 2                    | -  | -           | -                        | 10                     | Устный опрос<br>Тестирование<br>Подготовка реферата<br>Подготовка презентации<br>Выполнение проекта<br>Решение кейса |
| 4.    | Тема 4. Управление рисками   | 14                        | 2                               | -                                 | 2                    | -  | -           | -                        | 10                     | Устный опрос<br>Тестирование<br>Подготовка реферата<br>Подготовка презентации<br>Решение кейсов                      |
| 5.    | Тема 5. Управление инцидентами ИБ                                    | 14                        | 2                               | -                                 | 2                    | -  | -           | -                        | 10                     | Устный опрос<br>Тестирование<br>Подготовка реферата<br>Подготовка презентации  |



|    |   |            |           |          |           |          |          |          |           |  |
|----|---|------------|-----------|----------|-----------|----------|----------|----------|-----------|--|
|    |   |            |           |          |           |          |          |          |           | Решение кейса<br>Деловая игра  |
| 6. | Тема 6. Аудит ИБ  | 14         | 2         | -        | 2         | -        | -        | -        | 10        | Устный опрос<br>Тестирование<br>Подготовка реферата<br>Подготовка презентации<br>Решение кейса |
| 7. | Тема 7. Современные методы и средства анализа и управление рисками информационных систем компаний | 26         | 4         | -        | 2         | -        | -        | -        | 20        | Устный опрос<br>Тестирование<br>Подготовка реферата<br>Подготовка презентации                  |
| 8. | Зачет   | 2          | -         | -        | 2         | -        | -        | -        | 0         | -  |
| 9. | <b>ИТОГО:</b>   | <b>108</b> | <b>16</b> | <b>-</b> | <b>16</b> | <b>-</b> | <b>-</b> | <b>-</b> | <b>76</b> |  |

**Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

| <b>№ п/п</b>                                 | <b>Автор</b>     | <b>Название основной и дополнительной учебной литературы, необходимой для освоения дисциплины</b>   | <b>Выходные данные</b>   | <b>Количество экземпляров в библиотеке ДГУНХ/адрес доступа</b>  |
|--|------------------|---|--|---|
| <b>I. Основная учебная литература</b>        |                  |   |  |   |
| 1.   | Аверченков, В.И. | Аудит информационной безопасности : учебное пособие для вузов   | Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6            | <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=93245&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=93245&amp;sr=1</a>   |
| 2.   | Аверченков, В.И. | Служба защиты информации: организация и управление  | Москва : Издательство «Флинта», 2016. -186 с. ISBN 978-5-9765-1271-9                                 | <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=93356&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=93356&amp;sr=1</a>   |
| 3.   | Веселов, Г.Е.    | Менеджмент риска информационной безопасности  | Таганрог : Издательство Южного федерального университета, 2016. - 109 с.                             | <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=493331&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=493331&amp;sr=1</a> |
| 4.   | Пелешенко, В.С.  | Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления   | Ставрополь : СКФУ, 2017. - 86 с.   | <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=467139&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=467139&amp;sr=1</a> |
| <b>II. Дополнительная учебная литература</b> |                  |   |  |   |
| <b>A) Дополнительная учебная литература</b>  |                  |   |  |   |
| 1.   | -                | Аудит информационной безопасности органов исполнительной власти: учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыкин, М.В. Рудановский. | Москва : Издательство «Флинта», 2016. - 100 с. ISBN 978-5-9765-1277-1                                | <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=93259&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=93259&amp;sr=1</a>   |
| 2.   | Ковалев Д.В.     | Информационная безопасность   | Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. ISBN 978-5-9275-2364-1 | <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=493175&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=493175&amp;sr=1</a> |

|    |               |   |   |   |
|----|---------------|---|---|---|
| 3. | Нестеров С.А. | Основы информационной безопасности  | Санкт-Петербург : Издательство Политехнического университета, 2014. - 322 с. ISBN 978-5-7422-4331-1 | <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=363040&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=363040&amp;sr=1</a> |
| 4. | Пакин А.И.    | Информационная безопасность информационных систем управления предприятием | Москва : Альтаир : МГАВТ, 2009. - 41 с.   | <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=429778&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=429778&amp;sr=1</a> |

**Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ**

|    |   |  |  |  |
|----|---|--|--|--|
| 1. | Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).   |  |  |  |
| 2. | ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г.<br><a href="http://www.standartgost.ru">www.standartgost.ru</a>   |  |  |  |
| 3. | ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.<br><a href="http://www.standartgost.ru">www.standartgost.ru</a>   |  |  |  |
| 4. | ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г.<br><a href="http://www.standartgost.ru">www.standartgost.ru</a>  |  |  |  |
| 5. | ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»<br><a href="http://www.standartgost.ru">www.standartgost.ru</a>                           |  |  |  |
| 6. | ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.<br><a href="http://www.standartgost.ru">www.standartgost.ru</a> |  |  |  |
| 7. | ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»<br><a href="http://www.standartgost.ru">www.standartgost.ru</a>          |  |  |  |

**В) Периодические издания**

|    |   |  |  |  |
|----|---|--|--|--|
| 1. | Журнал для пользователей персональных компьютеров «Мир ПК»          |  |  |  |
| 2. | Научный журнал «Информатика и ее применение»                        |  |  |  |
| 3. | Информатика и безопасность  |  |  |  |
| 4. | Журнал о компьютерах и цифровой технике «Computer Bild»             |  |  |  |
| 5. | Рецензируемый научный журнал «Информатика и система управления»     |  |  |  |
| 6. | Рецензируемый научный журнал «Проблемы информационной безопасности» |  |  |  |

**Г) Справочно-библиографическая литература**

- |    |   |
|----|---|
| 1. | 1. Краткий энциклопедический словарь по информационной безопасности <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=58393&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=58393&amp;sr=1</a> |
|----|---|

## **Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета (<http://e-dgunh.ru>). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивает возможность доступа, обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

Для самостоятельного изучения материала и ознакомления с регламентирующими документами и текущей практикой в области менеджмента информационной безопасности, рекомендуется использовать следующие Интернет-ресурсы:

1. <http://www.fsb.ru/> – официальный сайт ФСБ
2. <http://fstec.ru/> – официальный сайт ФСТЭК
3. <http://www.consultant.ru/> – онлайн-версия информационно-правовой системы "КонсультантПлюс"
4. <http://Standartgost.ru> - Открытая база ГОСТов

## **Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных**

### **7.1. Необходимый комплект лицензионного программного обеспечения**

- Windows 10
- Microsoft Office Professional
- Adobe Acrobat Reader DC
- VLC Media player
- 7-zip
- Справочно-правовая система «КонсультантПлюс»

### **7.2. Перечень информационных справочных систем:**

- информационно справочная система «КонсультантПлюс».

### **7.3. Перечень профессиональных баз данных:**

- Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00>).
- Реестр операторов, осуществляющих обработку персональных данных (<https://rkn.gov.ru/personal-data/register/>);
- <http://Standartgost.ru> - Открытая база ГОСТов

## **Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Для преподавания дисциплины «Основы управления информационной безопасностью» используются следующие специальные помещения **и учебные аудитории:**

**Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 4.11** (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

### ***Перечень основного оборудования:***

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, персональный компьютер (моноблок) с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» ([www.biblioclub.ru](http://www.biblioclub.ru)), ЭБС «ЭБС Юрайт» ([www.urait.ru](http://www.urait.ru)).

### ***Перечень учебно-наглядных пособий:***

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

**Компьютерный класс, учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 4.2** (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

### ***Перечень основного оборудования:***

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, акустическая система.

Персональные компьютеры с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» ([www.biblioclub.ru](http://www.biblioclub.ru)), ЭБС «ЭБС Юрайт» ([www.urait.ru](http://www.urait.ru)) – 20 ед.

### ***Перечень учебно-наглядных пособий:***

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

**Помещение для самостоятельной работы № 4.5** (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

### ***Перечень основного оборудования:***

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 19 ед.

**Помещение для самостоятельной работы № 1-1** (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 1)

### ***Перечень основного оборудования:***

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 60 ед.

## **Раздел 11. Образовательные технологии**

При освоении дисциплины «Основы управления информационной безопасностью» используются следующие образовательные технологии:

- деловые и ролевые игры для выработки навыков принятия решения в случае инцидентов информационной безопасности;
- разбор конкретных ситуаций как для иллюстрации той или иной ситуации, так и в целях выработки навыков применения управленческих решений;
- проектная деятельность для выработки умений анализа информационных активов предприятия и разработки документов, регламентирующих деятельность по управлению информационной безопасностью в организации.
- внеаудиторная работа в форме обязательных консультаций и индивидуальных занятий со студентами (помощь в понимании тех или иных моделей и концепций, подготовка рефератов и эссе, а также тезисов для студенческих конференций и т.д.).

**Лист актуализации рабочей программы дисциплины  
«Основы управления информационной безопасностью»**

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от « 22 » май 2021 № 10

Зав. кафедрой В. Ганниб В. С.

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ № \_\_\_\_

Зав. кафедрой \_\_\_\_\_

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ № \_\_\_\_

Зав. кафедрой \_\_\_\_\_

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ № \_\_\_\_

Зав. кафедрой \_\_\_\_\_