



Основная профессиональная образовательная программа
02.03.02 Фундаментальная информатика и информационные технологии
(Фундаментальная информатика и информационные технологии)

Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Центр подготовки специалистов в сфере информационной безопасности и противодействия
техническим средствам разведки

ОДОБРЕНО:

Руководитель ОП

П.Г. Кононенко

(подпись)

«_1_» сентября_2022 г.

Рабочая программа дисциплины

Основы управления информационной безопасностью

| | |
|--|---|
| Уровень высшего образования: | бакалавриат |
| Квалификация выпускника: | бакалавр |
| Направление подготовки: | 02.03.02 Фундаментальная информатика и информационные технологии |
| Направленность (профиль) образовательной программы: | Фундаментальная информатика и информационные технологии |



1. Цели освоения дисциплины

Целью изучения дисциплины «Основы управления информационной безопасностью» являются получение необходимых знаний о принципах и методах, инструментальных средств, нормативных документах регуляторах, позволяющих успешно управлять информационной безопасностью организации в условиях активного использования информационных технологий.

2. Место дисциплины в структуре ОП

Настоящая дисциплина «Основы управления информационной безопасностью» относится к обязательной части учебного плана, изучается на 4-м курсе в 1 семестре. Курс опирается на следующие курсы: «Организационное и правовое обеспечение информационной безопасности», «Программно-аппаратные средства защиты информации» и «Методы и средства криптографической защиты информации».

3. Планируемые результаты обучения по дисциплине

3.1. Компетенции, формированию которых способствует дисциплина

При освоении дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

ОПК-5 Способен устанавливать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности

3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения формируемых компетенций

В результате освоения дисциплины обучающийся должен:

Знать:

- основные угрозы безопасности информации и модели нарушителя объекта информатизации;
- цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью;
- принципы формирования политики информационной безопасности объекта информатизации;

Уметь:

- разрабатывать модели угроз и модели нарушителя объекта информатизации;
- оценивать информационные риски объекта информатизации;
- обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей.

Иметь практический опыт/Иметь навыки:

- принципами и методами планирования, функционирования системы защиты информации;
- сущностью и содержанием контроля функционирования комплексной системы защиты информации.

4. Объем и содержание дисциплины

Объем дисциплины составляет 5 зачетных единиц (180 академических часов).

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа

Объем иной контактной работы и самостоятельной работы обучающегося по дисциплине указан в учебном плане образовательной программы.



Основная профессиональная образовательная программа
02.03.02 Фундаментальная информатика и информационные технологии
(Фундаментальная информатика и информационные технологии)

| № п/п | Разделы (темы) дисциплины | Семестр | Виды занятий, их объем (в ак. часах, по очной форме обучения) | | Формы текущего контроля успеваемости (по очной форме обучения) Формы промежуточной аттестации |
|----------|---|---------|---|-----------------------------------|---|
| | | | Занятия лекцион- ного типа | Занятия семинар- ского типа | |
| 1. | Вводный. Введение в проблематику дисциплины, представление рабочей программы, осмысление требований к организации процесса обучения, самостоятельной работы и форм аттестации | 7 | 1 | | Входная диагностика: тест с последующим обсуждением результатов. Список вопросов, интересующих студента по содержанию дисциплины (сдается в письменном виде) |
| 2. | Содержание и задачи процесса управления информационной безопасностью объекта информатизации. Система управления информационной безопасностью (ИБ) объекта информатизации. | 7 | 1 | 1 | Обсуждение результатов практической работы |
| 3. | Стандартизация в сфере управления ИБ (на основе международных стандартов ISO/IEC 17799, ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 15408). | 7 | 1 | 1 | Обсуждение результатов практической работы |
| 4. | Комплекс методов и средств защиты информации как объект управления ИБ. | 7 | 1 | 2 | Обсуждение результатов практической работы |
| 5. | Назначение и содержание политики ИБ организации в целом, его структурных подразделений, частных политик безопасности. Средства их реализации. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 6. | Модель нарушителя политики безопасности. Типичные угрозы информации и уязвимости корпоративных информационных систем. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 7. | Цели и задачи управления инцидентами ИБ. Системы управления инцидентами ИБ. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 8. | Этапы процесса управления инцидентами ИБ. Обнаружение, обработка событий и реагирование на события и инциденты ИБ. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 9. | Управление непрерывностью деятельности организации. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 10. | Системы защиты от внутренних угроз. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 11. | Обеспечение управления рисками информационной безопасности. Составляющие управления рисками. | 7 | 2 | 2 | Обсуждение результатов практической работы |



Основная профессиональная образовательная программа
02.03.02 Фундаментальная информатика и информационные технологии
(Фундаментальная информатика и информационные технологии)

| | | | | | |
|----------------------|---|---|----|----|--|
| 12. | Установление контекста управления рисками ИБ. Оценка рисков ИБ. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 13. | Назначение, цели и виды аудита ИБ. Требования к аудиту ИБ, особенности взаимодействия между аудитором и заказчиком. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 14. | Стандартизация в сфере аудита ИБ. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 15. | Содержание и организация процесса аудита ИБ. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 16. | Отчетные документы по результатам аудита. | 7 | 2 | 2 | Обсуждение результатов практической работы |
| 17. | Выполнение рекомендаций по итогам проведения аудита ИБ. | 7 | 1 | 2 | Обсуждение результатов практической работы |
| 18. | Заключительный. Подведение и анализ промежуточных результатов освоения дисциплины | 7 | 1 | 2 | Оценка контрольной работы |
| Итого за семестр: | | | 32 | 32 | Экзамен |
| Итого по дисциплине: | | | 32 | 32 | |

4.2. Развернутое описание содержания дисциплины по разделам (темам)

Содержание и задачи процесса управления информационной безопасностью объекта информатизации. Система управления информационной безопасностью (ИБ) объекта информатизации. Стандартизация в сфере управления ИБ (на основе международных стандартов ISO/IEC 17799, ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 15408). Комплекс методов и средств защиты информации как объект управления ИБ.

Назначение и содержание политики ИБ организации в целом, его структурных подразделений, частных политик безопасности. Средства их реализации. Модель нарушителя политики безопасности. Типичные угрозы информации и уязвимости корпоративных информационных систем.

Цели и задачи управления инцидентами ИБ. Системы управления инцидентами ИБ. Этапы процесса управления инцидентами ИБ. Обнаружение, обработка событий и реагирование на события и инциденты ИБ. Управление непрерывностью деятельности организации. Системы защиты от внутренних угроз.

Обеспечение управления рисками информационной безопасности. Составляющие управления рисками. Установление контекста управления рисками ИБ. Оценка рисков ИБ.

Назначение, цели и виды аудита ИБ. Требования к аудиту ИБ, особенности взаимодействия между аудитором и заказчиком. Стандартизация в сфере аудита ИБ. Содержание и организация процесса аудита ИБ. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита ИБ.

5. Образовательные технологии

Организация учебного процесса осуществляется в форме лекций, лабораторных занятий и индивидуальной самостоятельной работы студентов.

Учебный процесс по дисциплине «Основы управления информационной безопасностью» основан на использовании следующих инновационных образовательных технологий:

1. Технология проблемного обучения – основные темы курса на лекциях и лабораторных занятиях раскрываются через постановку и последующее разрешение проблемы создания алгоритма решения задачи и ее разрешение в виде функционирующей программы.



2. Технология тестового контроля качества образования – в процессе и по завершении теоретического обучения выполняется компьютерное тестирование.
3. Информационно-компьютерные технологии – применяются при выполнении лабораторных работ, самостоятельной внеаудиторной подготовке в виде самотестирования по сети Internet и использования учебных материалов в электронной форме.
4. Технология смешанного обучения.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Методика преподавания учебной дисциплины решает следующие основные задачи:

- определяет задачи обучения студентов по дисциплине;
- научно обосновывает содержание учебной программы, намечает последовательность ее изучения в комплексе с другими дисциплинами;
- определяет пути реализации принципов обучения при изучении дисциплины, формы и методы обучения;
- вырабатывает требования к методической подготовке преподавателей;
- изучает историю методики преподавания дисциплины;
- внедряет передовой опыт обучения;
- вырабатывает рекомендации по воспитанию обучаемых в процессе изучения дисциплины.

В соответствии с этими задачами осуществляется отбор научного материала, его систематизация и переработка в интересах развития и совершенствования содержания учебной дисциплины.

Методика разработана применительно к утвержденной рабочей программе для студентов с учетом требований Государственного образовательного стандарта высшего образования по направлению подготовки 02.03.01 «Фундаментальная информатика и информационные технологии», и вооружает преподавателей необходимыми знаниями, способствует их внедрению в практику обучения и воспитания студентов.

Выбор методов проведения занятий обусловлен учебными целями, содержанием учебного материала, временем, отводимым на занятия.

На занятиях в тесном сочетании применяется несколько методов, один из которых выступает ведущим. Он определяет построение и вид занятий.

На лекциях излагаются лишь основные, имеющие принципиальное значение и наиболее трудные для понимания и усвоения теоретические и практические вопросы.

Теоретические знания, полученные студентами на лекциях и при самостоятельном изучении курса по литературным источникам, закрепляются при выполнении лабораторных работ.

Целями проведения практических работ являются:

- приобретение практических навыков управления информационной безопасностью в организации;
- контроль самостоятельной работы студентов по освоению курса;
- обучение навыкам профессиональной деятельности.

Цели практических работ достигаются наилучшим образом в том случае, если им предшествует определенная подготовительная внеаудиторная работа. Поэтому преподаватель обязан довести до всех студентов график выполнения практических работ с тем, чтобы они могли заниматься целенаправленной самостоятельной работой.

Работы рекомендуется выполнять в той последовательности, в которой они написаны, потому что в некоторых работах используются элементы, полученные в предыдущей работе.

На занятиях со студентами должны широко использоваться разнообразные средства обучения, способствующие более полному и правильному пониманию темы лекции или практического занятия, а также выработке практических навыков по работе с ППО.

К средствам обучения студентов относятся:



- речь преподавателя;
- технические средства обучения: персональные компьютеры с установленным прикладным программным обеспечением;
- учебники, учебные пособия, лекции в электронном виде.

Полностью весь методический материал по обеспечению самостоятельной работы студентов приводится в Приложении 1 к РП.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Для контроля усвоения материала дисциплины «Основы управления информационной безопасностью» предусмотрен текущий и промежуточный контроль. Текущий контроль основан на анализе результатов выполнения практических работ и собеседовании по их темам. Промежуточный контроль заключается в сдаче экзамена по дисциплине.

Для проведения зачетов (экзаменов) в письменной или тестовой форме разрабатывается перечень вопросов, утверждаемый заведующим кафедрой. В перечень включаются вопросы из различных разделов курса, позволяющие проверить и оценить теоретические знания студентов и умение применять их для решения практических задач.

Зачет (экзамен) в письменной форме проводится одновременно для всех студентов академической группы. Время выполнения задания составляет не более одного академического часа.

При проведении зачета (экзамена) в письменной форме оценка выставляется на основе правил, принятых кафедрой, которые должны быть сообщены студентам до начала зачетной (экзаменационной) сессии.

Аналогичные правила могут быть заложены в программы компьютерного тестирования.

При контроле знаний в устной форме преподаватель использует метод индивидуального собеседования, в ходе которого обсуждает со студентом один или несколько вопросов из учебной программы. При необходимости могут быть предложены дополнительные вопросы, задачи и примеры. По окончании ответа на вопросы преподаватель объявляет студенту результаты сдачи зачета (экзамена).

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Ковалев, Д. В. Информационная безопасность : учебное пособие : [16+] / Д. В. Ковалев, Е. А. Богданова ; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=493175> (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.
2. Башлы, П. Н. Информационная безопасность: учебно-практическое пособие / П. Н. Башлы, Е. К. Баранова, А. В. Бабаши. – Москва : Евразийский открытый институт, 2011. – 375 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=90539> (дата обращения: 04.12.2022). – ISBN 978-5-374-00301-7. – Текст : электронный.
3. Артемов, А. В. Информационная безопасность: курс лекций / А. В. Артемов ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 257 с. : табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=428605> (дата обращения: 04.12.2022). – Текст : электронный.
4. Ефремов, И. В. Информационные технологии в сфере безопасности: практикум : учебное пособие / И. В. Ефремов, В. А. Солопова ; Оренбургский государственный университет. –



Оренбург : Оренбургский государственный университет, 2013. – 116 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=259178> (дата обращения: 04.12.2022). – Текст : электронный.

Дополнительная литература:

1. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=576726> (дата обращения: 04.12.2022). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

Система электронной поддержки образовательного процесса «Мой университет»
<https://uni.ivanovo.ac.ru>

Профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн» www.biblioclub.ru

Электронная библиотека ИвГУ <http://lib.ivanovo.ac.ru>

Электронный каталог НБ ИвГУ <http://lib.ivanovo.ac.ru/index.php/ek>

СПС «КонсультантПлюс» <http://www.consultant.ru/>

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и(или) LibreOffice, интернет-браузер Microsoft Edge и(или) Yandex Browser.

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

- для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения.

Лаборатория, оснащенная лабораторным оборудованием, комплектом специализированной учебной мебели и техническими средствами обучения.

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации:



Основная профессиональная образовательная программа
02.03.02 Фундаментальная информатика и информационные технологии
(Фундаментальная информатика и информационные технологии)

Автор(ы) рабочей программы дисциплины: Агупова Н.С., Зарубин И.А.

Программа рассмотрена и утверждена на заседании Центра подготовки специалистов в сфере информационной безопасности и противодействия техническим средствам разведки

« 1 » сентября 2022 г., протокол № 1

Программа обновлена
протокол заседания кафедры № _____ от « _____ » _____ 20 ____ г.

Согласовано:

Руководитель ОП _____ / _____

(подпись)

Программа обновлена
протокол заседания кафедры № _____ от « _____ » _____ 20 ____ г.

Согласовано:

Руководитель ОП _____ / _____

(подпись)