Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»

Кафедра аналитических и цифровых технологий

«Утверждаю»
Проректор по учебно-
методической работе
_____Ю.А. Устименко
«30» июня 2021 г.

Рабочая программа дисциплины
Б1.В.21 Информационная безопасность

Направление подготовки 38.03.01 Экономика
Направленность (профиль): Цифровая экономика
Форма обучения – заочная
Курс – 3
Семестр – 6
Всего зачетных единиц – 2, всего часов – 72
Лекции –4 час.
Лабораторные занятия – 6 час
Самостоятельная работа – 62 час.
Форма отчетности: зачет – 6 семестр

Программа составлена на основе ФГОС ВО направлению подготовки 38.03.01 Экономика.

Программу разработал:

кандидат физико-математических наук, доцент Д.С. Букачев.

Одобрена на заседании кафедры аналитических и цифровых технологий
«23» июня 2022 года, протокол № 10

Смоленск
2021

1. Место дисциплины в структуре ОП

Дисциплина «Информационной безопасности» является обязательной дисциплиной вариационной части образовательной программы по направлению подготовки 38.03.01 Экономика.

Изучение дисциплины предполагает сочетание фундаментальной подготовки с освоением технологии применения специализированных программных продуктов и систем, ориентированных на защиту экономической и служебной информации, базируется на компетенциях, сформированных при изучении дисциплин базовой части и по выбору таких, как «Цифровые платформы в экономике», «Интернет- технологии», «Электронный документооборот», «Интеллектуальные информационные системы в экономике».

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):

1) способностью использовать основы экономических знаний в различных сферах деятельности (ОК-3);
2) способность собрать и проанализировать исходные данные, необходимые для расчета экономических и социально-экономических показателей, характеризующих деятельность хозяйствующих субъектов (ПК-1).

В результате освоения дисциплины обучающийся должен

знать: цифровые инструменты и инфокоммуникационные технологии для идентификации, доступа к защищенной информации;

уметь: собирать и анализировать исходные данные для поиска организационно-управленческие решения по обеспечении сохранности данных;

владеть: навыками обеспечения защиты информации от различных угроз информационной безопасности; применять инфокоммуникационные технологии обеспечения идентификации и аудита событий информационных систем для решения профессиональных задач.

3. Содержание дисциплины

Тема 1. Теоретические основы информационной безопасности.

Понятие информационной безопасности. Составляющие информационной безопасности. Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Модели безопасности. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408.

Тема 2. Технологии и протоколы защиты информации в IP-сетях.

Протоколы IPSec и трансляция сетевых адресов. Межсетевые экраны. Протокол защиты электронной почты S/MIME. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей.

Тема 3. Анализ и управление рисками в сфере информационной безопасности.

Модель безопасности с полным перекрытием. Управление информационной безопасностью. Методики построения систем защиты информации. Модель Lifecycle Security. Модель многоуровневой защиты. Методика управления рисками, предлагаемая MS.

4. Тематический план

№ п/п	Разделы и темы	Всего часов	Формы занятий			
			Лекции	Практич. занятия	Лаборатор. занятия	Самостоя-тельная работа
1.	Теоретические основы информационной безопасности	16	0	0	0	16
2.	Технологии и протоколы защиты информации в IP-сетях	26	2	0	2	22
3.	Анализ и управление рисками в сфере информационной безопасности	26	2	0	4	20
	Подготовка к зачету	4				4
	Всего за семестр	72	4	0	6	62

5. Виды учебной деятельности

Лекции

Лекция 1.

Понятие информационной безопасности. Составляющие информационной безопасности. Общая схема процесса обеспечения безопасности. Уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ.

Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа.

Модели безопасности. Процесс построения и оценки системы обеспечения безопасности. Концепции стандарта ISO/IEC 15408.

Лекция 2.

Сетевые протоколы IPSec и трансляция сетевых адресов. Технологии создания межсетевых экранов при передаче данных.

Протокол защиты электронной почты S/MIME. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей.

Модель безопасности с полным перекрытием. Управление информационной безопасностью.

Методики построения систем защиты информации. Модель Lifecycle Security.

Модель многоуровневой защиты. Методика управления рисками, предлагаемая MS.

Лабораторные занятия

Задания к лабораторным работам с подробными методическими рекомендациями и дополнительные материалы к лабораторным занятиям представлены в виде информационного контента на образовательном сервере **http://cdo.smolgu.ru**.

Лабораторная работа №1. Настройка политики безопасности и управление доступом к объектам файловой системы **(2 часа).** Цель работы: приобретение практических навыков по настройке разрешений на доступ к файлам в операционных системах семействах Windows.

Задание 1.

Произведите настройки приложения Проводник для эффективной работы с NTFS.

Определите права доступа пользователей к объектам диска.

Создайте папку с именем, соответствующим Вашей фамилии, на диске С. Для данной папки установите права доступа таким образом, чтобы только пользователь Student имел возможность просматривать и редактировать объекты папки.

Создайте нового пользователя системы с именем «ЛР» (Пуск – Панель управления – Учётные записи пользователей). Установите пароль для пользователя: 2.

Авторизуйтесь в системе от имени пользователя «ЛР». Попробуйте получить доступ к папке с именем, соответствующим Вашей фамилии, на диске С.

Авторизуйтесь в системе от имени пользователя «Студент». Для папки с именем, соответствующим Вашей фамилии, в Моих документах установите права доступа таким образом, чтобы все пользователи имели возможность просматривать и редактировать объекты папки.

Авторизуйтесь в системе от имени пользователя «ЛР». Попробуйте получить доступ к папке с именем, соответствующим Вашей фамилии, в Моих документах.

Авторизуйтесь в системе от имени пользователя «Студент». Удалите пользователя «ЛР» из системы.

Задание 2 (*для самостоятельного выполнения*).

Изучите управление политиками аудита безопасности в системе Windows. Управление политиками аудита можно осуществлять через оснастку «Локальные параметры безопасности». Для вызова оснастки «Локальные параметры безопасности» нажмите Пуск - Выполнить, наберите secpol.msc и нажмите ОК. Далее выберите «Локальные политики» - «Политика аудита».

Изучите аудит событий Windows и объектов файловой системы. После выбора политики аудита, изучение процесса аудита следует осуществлять экспериментальным путем в два этапа:

- выполнение действия, подлежащего аудиту (например, добавление новой учетной записи при включенной политике «Аудита управления учетными записями»);
- просмотр зарегистрированного события в журнале безопасности Windows.

При включении соответствующей политики аудита, регистрация событий аудита начинается автоматически. Это справедливо для всех политик аудита, кроме «Политики аудита доступа к объектам».

Для просмотра и управления журналом безопасности Windows используют оснастку «Просмотр событий». Для вызова оснастки необходимо: нажать Пуск > Выполнить и набрать eventvwr.msc и нажать ОК

Лабораторная работа №2. Сбор данных об информационной системе с помощью средств администрирования Windows и выявление уязвимостей системы **(2 часа).** Цель работы: приобретение навыков по сбору и анализу данных об имеющихся компьютерах, установленных на них операционных системах, предоставляемых в общий сетевой доступ файловых ресурсах.

Задание 1.

Получите перечень компьютеров локальной сети. Для своего и соседнего компьютеров определите: Имя компьютера, IP-адрес и MAC-адрес.

Получите перечень предоставляемых в общий доступ ресурсов на вашем компьютере и на компьютере. Опишите хранимые там данные и охарактеризуйте степень их полезности и конфиденциальности.

Для указанных ресурсов и опишите действующие разрешения на доступ. При этом надо учитывать, что:

- эффективное (действующее) разрешение складывается из разрешений для пользователя лично и разрешений всех групп, в которые пользователь входит;
- запрещение имеет больший приоритет, чем разрешение;
- при комбинации разрешений для общего ресурса с разрешениями NTFS, приоритетными будут разрешения, максимально ограничивающие доступ.

Перечислите все активные сетевые соединения на своём компьютере с информацией об именах исполняемых файлов.

Определите DNS СДО СмолГУ. Постройте маршрут пакетов от Вашего компьютера до СДО СмолГУ.

Задание 2 (*для самостоятельного выполнения*).

С помощью утилиты NetView просканировать локальную сеть, определить IP, MAC, ресурсы общего доступа, учётные записи пользователей своего и соседнего компьютера.

Выполните проверку Вашего компьютера с помощью Microsoft Baseline security analyzer. Укажите:

– как оценен уровень уязвимости Вашего компьютера;

– какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей;

– опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере.

Проведите анализ результатов. Какие уязвимости можно устранить, какие – нельзя из-за особенностей конфигурации ПО или использования компьютера?

Выполните удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.

Опишите действующую на вашем компьютере политику паролей. Если в ходе проверки утилитой BSA были выявлены уязвимости связанные с управлением паролями пользователей, опишите пути их устранения или обоснуйте необходимость использования действующих настроек.

Лабораторная работа №3. Анализ и управление рисками **(2 часа).** Цель работы: приобретение практических навыков по выявлению рисков в информационных системах и управлению настроек программных средств по их снижению.

Задание 1.

Проведите сканирование своего и соседнего компьютеров в учебной лаборатории. При сканировании надо учитывать, что часть имеющихся уязвимостей может быть закрыта путем использования встроенного межсетевого экрана (брандмауэра Windows). Чтобы получить более полную информацию об исследуемых узлах, лучше провести одно сканирование при включенном, другое - при отключенном межсетевом экране (изменение настройки доступно через Панель управления -> Брандмауэр Windows). Аналогичная ситуация возникает и при использовании других межсетевых экранов.

Опишите результаты проверки – полученные данные о компьютере и сетевых службах, наиболее серьезные из обнаруженных уязвимостей и пути их устранения. Охарактеризуйте уровень безопасности проверенных компьютеров. При анализе результатов сканирования используйте техническую статью «Службы и сетевые порты в серверных системах Microsoft Windows», доступную по ссылке http://support.microsoft.com/?kbid=832017.

Проведите сканирование домена smolgu.ru. Опишите результаты проверки – полученные данные о компьютере и сетевых службах, наиболее серьезные из обнаруженных уязвимостей и пути их устранения. Охарактеризуйте уровень безопасности проверенных компьютеров. При анализе результатов сканирования используйте техническую статью «Службы и сетевые порты в серверных системах Microsoft Windows», доступную по ссылке http://support.microsoft.com/?kbid=832017.

Просканируйте Ваш компьютер с помощью сервисов сканирования настроек безопасности и опишите результаты проверки:

http://portscan.ru/portscanner.html

http://www.testip.ru/services/portscan.html

https://2ip.ru/port-scaner/

Задание 2.

Составьте бизнес-модель компании, которая активно использует компьютерную технику, сетевое оборудование, информационные технологии и системы в своей деятельности. Уделите особое внимание мерам по обеспечению информационной безопасности на предприятии и расходам на их реализацию.

Подробно опишите реально существующее или вымышленное малое предприятие (до 1000 сотрудников): сферу деятельности, состав и структуру информационной системы, особенности организации процесса защиты информации, применяемые методы и средства и т.д.

С помощью программы MSAT проведите оценку рисков для предприятия. Сформируйте и сохраните полный и расширенный отчеты MSAT.

Задание 3 (*для самостоятельного выполнения*)

Просмотрите параметры сертификата «Сбербанк Онлайн» Сбербанка – https://online.sberbank.ru/CSAFront/index.do. Сделайте скриншот, опишите, кем, на какой срок и для какого субъекта сертификат был выдан.

Выявите процесс хранения сертификатов в ОС Windows. Операционная система Windows обеспечивает защищенное хранилище ключей и сертификатов. Работать с хранилищем можно используя настройку консоль управления MMC «Сертификаты».

Из меню Пуск -> Выполнить запустите консоль командой mmc. В меню Консоль выберите Добавить или удалить оснастку, а в списке оснасток выберите Сертификаты. Если будет предложен выбор (а это произойдет, если Вы работаете с правами администратора), выберите пункт «Моей учетной записи».

В разделе «Доверенные корневые центры сертификации» представлен достаточно обширный список центров, чьи сертификаты поставляются вместе с операционной системой.

Найдите в нем сертификат VeriSign Class 3 Public Primary CA. Благодаря тому, что он уже был установлен, в рассмотренном в начале работы примере с подключением к системам Интернет-банкинга браузер мог подтвердить подлинность узла.

Самостоятельная работа

Задания для самостоятельного выполнения разбиты в соответствии с тематическим планированием курса и являются гармоничным дополнением к лабораторным работам (см. пункт «Виды учебной деятельности. Лабораторные занятия»).

Вопросы для самостоятельного изучения по дисциплине

Тема 1.

1. В чем заключается проблема «информационной безопасности»?
2. Дайте определение «информационной безопасности».
3. Перечислите составляющие информационной безопасности и их определение.
4. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
5. Перечислите уровни формирования режима информационной безопасности.
6. Перечислите основополагающие документы по «информационной безопасности».
7. Основные задачи «информационной безопасности» в соответствии с Концепцией национальной безопасности РФ.
8. Какие виды требований включает стандарт ISO/IEC 15408?
9. Дайте характеристику составляющих «информационной безопасности» применительно к вычислительным сетям.
10. Перечислите основные механизмы безопасности.
11. Что понимается под администрированием средств безопасности?
12. Классы защищенности межсетевых экранов.

13. Содержание административного уровня обеспечения «информационной безопасности».
14. На чем основан механизм регистрации?
15. Какие события, связанные с безопасностью, подлежат регистрации?
16. Чем отличаются механизмы регистрации и аудита?
17. Какие этапы предусматривают механизмы регистрации и аудита?
18. Дайте определение политики безопасности.
19. Направления разработки политики безопасности.
20. Перечислите классы угроз информационной безопасности.
21. Назовите причины и источники случайных воздействий на информационные системы.
22. Дайте характеристику преднамеренным угрозам.
23. Перечислите каналы несанкционированного доступа.
24. Что понимается под техническим каналом утечки информации?
25. Каковы причины возникновения электромагнитных каналов утечки информации?
26. Как образуется параметрический канал утечки информации?
27. Основные угрозы целостности информации.
28. Охарактеризуйте угрозы доступности информации.

Тема 2.

1. Каковы характерные черты компьютерных вирусов?
2. Дайте определение программного вируса.
3. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
4. Перечислите классификационные признаки компьютерных вирусов.
5. В чем особенности резидентных вирусов?
6. Перечислите деструктивные возможности компьютерных вирусов.
7. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
8. Перечислите виды «вирусоподобных» программ.
9. Поясните механизм функционирования «троянской программы» (логической бомбы).
10. Поясните понятия «сканирование на лету» и «сканирование по запросу».
11. Перечислите виды антивирусных программ.
12. Охарактеризуйте антивирусные сканеры.
13. В чем особенности эвристических сканеров?
14. Какие факторы определяют качество антивирусной программы?
15. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
16. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
17. Характерные черты макровируса.
18. Как проверить систему на наличие макровируса?
19. В чем заключаются особенности обеспечения «информационной безопасности» компьютерных сетей?
20. Дайте определение понятия «удаленная угроза».
21. В чем заключается специфика методов и средств защиты компьютерных сетей?
22. Поясните понятие «глобальная сетевая атака», приведите примеры.
23. Какие протоколы образуют модель TCP/IP?
24. Какой протокол обеспечивает преобразование логических сетевых адресов в аппаратные?

25. Проведите сравнительную характеристику моделей передачи данных TCP/IP и OSI/ISO.

26. На каком уровне модели OSI/ISO реализуется сервис безопасности «неотказуемость» (согласно «Общим критериям»)?

27. Для чего предназначен DNS-сервер?

28. Перечислите классы удаленных угроз.

29. Как классифицируются удаленные угрозы «по характеру воздействия»?

30. Охарактеризуйте удаленные угрозы «по цели воздействия».

31. Может ли пассивная угроза привести к нарушению целостности информации?

32. Дайте определение типовой удаленной атаки.

33. Что является целью злоумышленников при «анализе сетевого трафика»?

34. Назовите причины успеха удаленной атаки «ложный объект».

Тема 3.

1. Что понимается под идентификацией и аутентификацией пользователя?

2. Перечислите возможные идентификаторы при реализации механизмов идентификации и аутентификации.

3. Что такое «электронный ключ»?

4. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?

5. Что входит в состав криптосистемы?

6. Как реализуются симметричный и асимметричный методы шифрования?

7. Что такое электронная цифровая подпись?

8. Перечислите методы разграничения доступа.

9. Какие методы управления доступом предусмотрены в руководящих документах Гостехкомиссии?

10. В чем заключается принцип межсетевого экранирования?

11. Принцип функционирования межсетевых экранов с фильтрацией пакетов.

12. Какие сервисы безопасности включает технология виртуальных частных сетей?

13. Почему при использовании технологии VPN IP-адреса внутренней сети недоступны внешней сети?

14. Чем определяется политика безопасности виртуальной частной сети?

6. Фонд оценочных средств

Компетенция	Этапы формирования (семестр)	Дисциплины, практики, НИР, ГИА	Критерии	Показатели (по уровням)
ОК-3 способность использовать основы экономических знаний в различных сферах деятельности	**6**	**Б1.В.21 Информационная безопасность**	**Знаниевый**	**«Зачтено»** ***знает*** цифровые инструменты и инфокоммуникационные технологии для идентификации, доступа к защищенной информации **«Не зачтено»** ***не знает*:** цифровые инструменты и инфокоммуникационные технологии для идентификации, доступа к защищенной информации
			Деятельностный	**«Зачтено»** ***умеет*:** собирать и анализировать исходные данные для поиска организационно-управленческие решения по обеспечении сохранности данных ***владеет*:** навыками обеспечения защиты информации от различных угроз информационной безопасности; применять инфокоммуникационные технологии обеспечения идентификации и аудита событий информационных систем для решения профессиональных задач **«Не зачтено»** ***не умеет:*** собирать и анализировать исходные данные для поиска организационно-управленческие решения по обеспечении сохранности данных ***не владеет:*** навыками обеспечения защиты информации от различных угроз информационной безопасности; применять инфокоммуникационные технологии обеспечения идентификации и аудита событий информационных систем для решения профессиональных задач

ПК-1 способность собрать и проанализировать исходные данные, необходимые для расчета экономических и социально-экономических показателей, характеризующих деятельность хозяйствующих субъектов	**6**	**Б1.В.21 Информационная безопасность**	**Знаниевый**	**«Зачтено»** ***знает*** цифровые инструменты и инфокоммуникационные технологии для идентификации, доступа к защищенной информации **«Не зачтено»** ***не знает*:** цифровые инструменты и инфокоммуникационные технологии для идентификации, доступа к защищенной информации
			Деятельностный	**«Зачтено»** ***умеет*:** собирать и анализировать исходные данные для поиска организационно-управленческие решения по обеспечении сохранности данных ***владеет*:** навыками обеспечения защиты информации от различных угроз информационной безопасности; применять инфокоммуникационные технологии обеспечения идентификации и аудита событий информационных систем для решения . профессиональных задач **«Не зачтено»** ***не умеет:*** собирать и анализировать исходные данные для поиска организационно-управленческие решения по обеспечении сохранности данных ***не владеет:*** навыками обеспечения защиты информации от различных угроз информационной безопасности; применять инфокоммуникационные технологии обеспечения идентификации и аудита событий информационных систем для решения профессиональных задач

Оценочные средства
(примеры)

Вопросы для самостоятельного изучения

Вопросы для самостоятельного изучения указаны в пункте «Виды учебной деятельности. Самостоятельная работа».

Критерии оценивания ответов на вопросы для самостоятельного изучения

Ответ по каждому вопросу оценивается по пятибалльной шкале в зависимости от содержательности ответа и логики изложения материала.

Уровень ответа	Оценка
Полно и аргументировано отвечает по содержанию темы; может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из лекции, но и самостоятельно составленные; излагает материал последовательно и корректно.	5 (отлично)
Дает ответ, удовлетворяющий тем же требованиям, что и для оценки «5», но допускает 1-2 ошибки, которые сам же исправляет.	4 (хорошо)
Излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки.	3 (удовлетворительно)
Не знает ответ на вопрос, допускает существенные ошибки в формулировке определений и алгоритмов, искажающие их смысл, беспорядочно и неуверенно излагает материал.	2 (неудовлетворительно)

Задания для самостоятельного выполнения

Задания для самостоятельного выполнения разбиты в соответствии с тематическим планированием курса и являются гармоничным дополнением к лабораторным работам (см. пункт «Виды учебной деятельности. Лабораторные занятия»).

Критерии оценивания заданий для самостоятельного выполнения.

Уровень выполнения	Оценка
Задача решена в полном объёме, алгоритмические и вычислительные ошибки отсутствуют, проведен анализ полученного решения.	5 (отлично)
Задача решена в полном объёме с незначительными техническими ошибками или отсутствует анализ результатов решения.	4 (хорошо)
Задача решена не полностью или в решении присутствуют ошибки алгоритмического характера, незначительно влияющие на ход решения.	3 (удовлетворительно)
Задача не решена или в решении присутствует значительное количество ошибок алгоритмического характера, существенно влияющих на ход решения.	2 (неудовлетворительно)

Критерии получения зачета

Зачет выставляется по результатам работы студента в течение семестра согласно Положению о текущем контроле успеваемости и промежуточной аттестации студентов в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Смоленский государственный университет».

Для получения зачета студент должен:

- выполнить задания лабораторных работ на оценку не ниже «удовлетворительно»;
- выполнить задания для самостоятельной работы на оценку не ниже «удовлетворительно»;
- уметь отвечать на вопросы для самостоятельного изучения на оценку не ниже «удовлетворительно».

7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети Интернет

Список основной литературы

1. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/444046
2. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171
3. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433715
4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966
5. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации».
6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
7. ГОСТ Р ИСО/МЭК 15408-2-2013. Национальный стандарт Российской Федерации (ISO/IEC-15408).
8. Федеральная служба по техническому и экспортному контроля России. Техническая защита информации. Документы. Национальные документы. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty

Список дополнительной литературы

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и

магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966
2. Галатенко В. Основы информационной безопасности. Национальный открытый университет ИНТУИТ. URL: https://www.intuit.ru/studies/courses/10/10/info (дата обращения 10.10.2019).
3. Граничин О., Князев В. Безопасность информационных систем. Национальный открытый университет ИНТУИТ. URL: https://www.intuit.ru/studies/courses/13845/1242/info

.

Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Свободно доступные курсы Интернет-университета информационных технологий (ИНТУИТ) http://www.intuit.ru/;
2. Портал государственных и муниципальных услуг. http://www.gosuslugi.ru/;
3. Официальный сайт ЗАО «Консультант Плюс» – www.consultant.ru;
4. Официальный сайт ООО «НПП Гарант-Сервис» – www.garant.ru;

8. Методические указания для обучающихся по освоению дисциплины

1. Мультимедийные презентации PowerPoint для проведения лекций.
2. Комплексы лабораторных работ, представленные в виде информационного контента.

Электронные материалы размещены на образовательном сервере СмолГУ **http://cdo.smolgu.ru**.

9. Перечень информационных технологий

Kaspersky Endpoint Security для бизнеса Стандартный АО «Лаборатория Касперского».
Microsoft Open License в составе:

– Microsoft Windows Professional XP, 7, 8 Server Russian;

– Microsoft Office 2003-2016 Russian.

10. Материально-техническая база

Учебная аудитория для проведения занятий лекционного типа. Аудитория 124 уч.к. № 2.

Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.

Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 18 шт., колонки Genius – 18 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.

Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).

Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – компьютерный класс. Аудитория 124 уч.к. №2.

Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.

Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 16 шт., колонки Genius – 16 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.

Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).

Помещение для самостоятельной работы – компьютерный класс с доступом к сети «Интернет» и ЭИОС СмолГУ. Аудитория 124 уч.к. №2.

Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.

Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 18 шт., колонки Genius – 18 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.

Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).