Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Нижегородский институт управления – филиал РАНХиГС
(наименование института (факультета))
Кафедра информатики и информационных технологий
(наименование кафедры)

УТВЕРЖДЕНО
Директор Нижегородского института управления – филиала РАНХиГС

ПРОГРАММА БАКАЛАВРИАТА

Корпоративные информационные системы управления

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
реализуемой с применением электронного (онлайн) курса

Б1.О.21 ИФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
(индекс и наименование дисциплины (модуля), в соответствии с учебным планом)

направление подготовки
09.03.03 Прикладная информатика
(код и наименование направления подготовки)

очная, заочная
(форма(ы) обучения)

2024
(год набора)

Нижний Новгород, 2024 г.

Автор-составитель:

Доцент кафедры информатики и информационных технологий, кандидат физико-математических наук, доцент *(ученая степень и(или) ученое звание, должность, наименование кафедры)*	В.И. Окулич *(Ф.И.О.)*
Заведующий кафедрой информатики и информационных технологий, кандидат технических наук, доцент *(ученая степень и(или) ученое звание, должность, наименование кафедры)*	И.И. Гребенюк *(Ф.И.О.)*
Заведующий кафедрой информатики и информационных технологий, кандидат технических наук, доцент *(ученая степень и(или) ученое звание, должность, наименование кафедры)*	И.И. Гребенюк *(Ф.И.О.)*

Изменения РПД Б1.О.21 «Информационная безопасность» одобрены на заседании кафедры информатики и информационных технологий

Протокол от 20 февраля 2024 г. № 12.

Содержание

1. **Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы** 4

2. **Объем и место дисциплины в структуре ОП ВО** 4

3. **Содержание и структура дисциплины** 5

4. Материалы текущего контроля успеваемости обучающихся 7

5. Оценочные материалы промежуточной аттестации по дисциплине 15

6. Методические материалы по освоению дисциплины с применением ЭК 18

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет 21

7.1 Основная литература 21

7.2 Дополнительная литература 21

7.3 Учебно-методическое обеспечение самостоятельной работы. 21

7.4 Нормативные правовые документы 22

7.5. Интернет-ресурсы 24

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 24

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1 Дисциплина «Информационная безопасность» обеспечивает овладение следующими компетенциями:

Таблица 1

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента освоения компетенции
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2	Способен применять различные поисковые системы, электронные библиотеки и базы знаний при решении задач профессиональной деятельности
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.2	Способен принимать участие в разработке технической документации на различных этапах жизненного цикла информационной системы в рамках совместного группового проекта, связанного с профессиональной деятельностью

1.2. Студенты также должны овладеть навыками:

- владения методами решения стандартных задач профессиональной деятельности, средствами обеспечения информационной безопасности;
- составления технической документации на различных этапах жизненного цикла информационной системы.

2. Объем и место дисциплины в структуре ОП ВО

Индекс дисциплины Б1.О.21 «Информационная безопасность» является дисциплиной обязательной части образовательной программы.

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 академических часа / 81 астрономический час.

По очной форме обучения: количество академических часов, выделенных на контактную работу с преподавателем составляет 48 часов, из них, лекции - 16 часов, практические занятия - 32 часов. Самостоятельная работа составляет - 56 часов, контроль – 4 часа.

По заочной форме обучения: количество академических часов, выделенных на контактную работу с преподавателем составляет 12 часов, из них, лекции – 4 часа, практические занятия – 8 часов. Самостоятельная работа составляет 92 часов, контроль – 4 часов.

Форма промежуточной аттестации в соответствии с учебным планом: зачет с оценкой.

3. Содержание и структура дисциплины

3.1 Структура дисциплины

Таблица 2

№ п/п	*Наименование тем (разделов)*	*Объем дисциплины, час.*						*Форма текущего контроля успеваемости и промежуточной аттестации*
		Всего	*Контактная работа обучающихся с преподавателем по видам учебных занятий*				*СР*	
			*Л/ЭО, ДОТ**	*ЛР/ ЭО, ДОТ**	*ПЗ/ ЭО, ДОТ**	*КСР*		
Очная форма обучения								
Тема 1	Введение в проблематику информационной безопасности	14	2		4		8	О, Пз, ЛР
Тема 2	Угрозы информационной безопасности	16	2		6		8	О, Пз, ЛР
Тема 3	Вредоносные программы и противодействие им	14	2		4		8	О, Пз, ЛР
Тема 4	Методы и средства защиты компьютерной информации.	14	2		4		8	О, Пз, ЛР
Тема 5	Криптографические методы информационной безопасности.	16	4		4		8	О, Пз, ЛР
Тема 6	Лицензирование и сертификация в области защиты информации	14	2		4		8	О, Пз, ЛР
Тема 7	Критерии информационной безопасности, оценки рисков и управление её обеспечением.	16	2		6		8	О, Пз, ЛР
Промежуточная аттестация								Зачет с оценкой
Всего (в з.е./акад.часах/астр.часах):		**3/108 /81**	**16/12**		**32/24**		**56/42**	**4/3**
Заочная форма обучения								
Тема 1	Введение в проблематику информационной безопасности	16	2		2		12	О, Пз, ЛР
Тема 2	Угрозы информационной безопасности	13			1		12	О, Пз, ЛР
Тема 3	Вредоносные программы и противодействие им	15			1		14	О, Пз, ЛР
Тема 4	Методы и средства защиты компьютерной информации.	14			1		13	О, Пз, ЛР
Тема 5	Криптографические методы информационной безопасности.	14			1		13	О, Пз, ЛР
Тема 6	Лицензирование и	18	2				15	О, Пз, ЛР

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости и промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО, ДОТ*	ЛР/ ЭО, ДОТ*	ПЗ/ ЭО, ДОТ*	КСР		
	сертификация в области защиты информации				1			
Тема 7	Критерии информационной безопасности, оценки рисков и управление её обеспечением.	14			1		13	О, Пз, ЛР
Промежуточная аттестация		4						Зачет с оценкой
Всего (в з.е./акад.часах/астр.часах):		**3/108 /81**	**4/3**		**8/6**		**92/69**	**4/3**

Примечание:

** – при применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом*

*** – формы текущего контроля успеваемости: опрос (О), тестирование (Т),), оценка доклада (Д), оценка работы с документами в микрогруппе (М), оценка презентации(Пр), отчет по практическим занятиям (Пз), отчет по лабораторным работам (Лб) .*

3.2 Содержание дисциплины

Тема 1. Введение в проблематику информационной безопасности

Понятие и связь национальной и информационной безопасностей. Место информационной безопасности (ИБ) в системе национальной безопасности РФ. Доктрина ИБ, История проблемы ИБ, угрозы ИБ. Комплексный подход к обеспечению информационной безопасности. Основные понятия защиты информации. Организационно-правовое обеспечение информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Политика информационной безопасности.

Тема 2. Угрозы информационной безопасности.

Понятие угрозы для информации. Классификация угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.). Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Действия и события, нарушающие информационную безопасность. Способы воздействия угроз на информационные объекты.

Тема 3. Вредоносные программы и противодействие им.

Обязательные условия вредоносности. Разновидности вредоносных программ. Клавиатурные перехватчики. «Логические бомбы». Сетевые «черви». «Жадные» программы. Программы «глюки». Программы-шпионы и компьютерные закладки. Захват ресурсов компьютера.

Признаки заражения вирусом. Ответственность за распространение вредоносных программ.. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Защита данных и сервисов от воздействия вредоносных программ. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.

Тема 4. Методы и средства защиты компьютерной информации.

Общее представление о структуре защищенной информационной системы Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым

ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.

Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах.

Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.

Тема 5. Криптографические методы информационной безопасности.

Основные понятия криптологии. Симметричные и ассиметричные криптосистемы. Способы создания симметричных криптосистем. Абсолютно стойкий шифр. Криптографическая система DES и её модификации. Алгоритм криптографического преобразования по ГОСТ 28147-89. Принципы построения ассиметричных криптографических систем.

Тема 6. Лицензирование и сертификация в области защиты информации.

Правовая основа системы лицензирования и сертификации в РФ. Виды деятельности в информационной сфере, подлежащие лицензированию. Лицензирование деятельности по защите информации. Объекты лицензирования в сфере защиты информации. Органы лицензирования и их полномочия. Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области защиты информации. Объекты сертификационной деятельности. Органы сертификации и их полномочия. Система государственного обеспечения информационной безопасности в Российской Федерации.

Тема 7. Критерии информационной безопасности, оценки рисков и управление её обеспечением.

Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Основные понятия, механизмы безопасности, классы безопасности. Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности, сетевые механизмы безопасности, администрирование средств безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий. Руководящие документы Гостехкомиссии и ФСТЭК РФ.

4. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 3.

№	Тема (раздел)	Методы текущего контроля успеваемости
Тема 1	Введение в проблематику информационной безопасности	Опрос, отчет по практическим занятиям и лабораторным работам
Тема 2	Угрозы информационной безопасности.	Опрос, отчет по практическим занятиям и лабораторным работам
Тема 3	Вредоносные программы и противодействие им.	Опрос, отчет по практическим занятиям и лабораторным работам
Тема 4	Методы и средства защиты компьютерной информации.	Опрос, отчет по практическим занятиям и лабораторным работам
Тема 5	Криптографические методы информационной безопасности.	Опрос, отчет по практическим занятиям и лабораторным работам

№	Тема (раздел)	Методы текущего контроля успеваемости
Тема 6	Лицензирование и сертификация в области защиты информации.	Опрос, отчет по практическим занятиям и лабораторным работам
Тема 7	Критерии информационной безопасности, оценки рисков и управление её обеспечением.	Опрос, отчет по практическим занятиям и лабораторным работам

4.2. Типовые материалы текущего контроля успеваемости обучающихся

4.2.1. Вопросы для самостоятельной подготовки к практическим занятиям по темам дисциплины и последующего опроса

Тема 1 «*Введение в проблематику информационной безопасности* »

Вопросы опроса по теме:

- В чём сущность комплексного подхода к защите информации?
- Каковы основные характеристики защищаемой информации?
- Что включает в себя политика безопасности?
- В чём сущность организационной защиты информации?
- Какие законодательные акты составляют основу российского информационного права?
- Что относится к средствам инженерно-технической защиты информации и для чего они предназначены?
- В чём заключаются достоинства и недостатки программных средств защиты информации?
- Какие существуют международные и российские стандарты в области информационной безопасности?

Примерное содержание практического занятия по теме:

Задание на лабораторную работу

Пусть множество *S* возможных операций над объектами компьютерной системы задано следующим образом: *S* = {«Доступ на чтение», «Доступ на запись», «Передача прав»}.

1. Получить данные о количестве пользователей и объектов компьютерной системы из табл. 2, соответственно варианту.

2. Реализовать программный модуль, создающий матрицу доступа пользователей к объектам компьютерной системы. Реализация данного модуля подразумевает следующее:

2.1. Необходимо выбрать идентификаторы пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей указано для варианта). Например, множество из трёх идентификаторов пользователей {Ivan, Sergey, Boris}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами доступа ко всем объектам).

2.2. Реализовать программное заполнение матрицы доступа, содержащей количество пользователей и объектов, соответственно Вашему варианту.

2.2.1. При заполнении матрицы доступа необходимо учитывать, что один из пользователей должен являться администратором системы (допустим, Ivan). Для него права доступа ко всем объектам должны быть выставлены как полные.

2.2.2. Права остальных пользователей для доступа к объектам компьютерной системы должны заполняться случайным образом с помощью датчика случайных чисел. При заполнении матрицы доступа необходимо учитывать, что пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав.

2.2.3. Реализовать программный модуль, демонстрирующий работу в дискреционной модели политики безопасности.

3. Данный модуль должен выполнять следующие функции:

3.1. При запуске модуля должен запрашиваться идентификатор пользователя (проводится идентификация пользователя), при успешной идентификации пользователя должен осуществляться вход в систему, при неуспешной – выводиться соответствующее сообщение.

3.2. При входе в систему после успешной идентификации пользователя на экране должен распечатываться список всех объектов системы с указанием перечня всех доступных прав доступа идентифицированного пользователя к данным объектам. Вывод можно осуществить, например, следующим образом:

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Чтение

Объект2: Запрет

Объект3: Чтение, Запись

Объект4: Полные права

Жду ваших указаний >

3.3. После вывода на экран перечня прав доступа пользователя к объектам компьютерной системы, необходимо организовать ожидание указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя, на экран необходимо вывести сообщение об успешности либо не успешности операции. При выполнении операции передачи прав (grant) должна модифицироваться матрица доступа. Программа должна поддерживать операцию выхода из системы (quit), после которой запрашивается идентификатор пользователя. Диалог можно организовать, например, так:

Жду ваших указаний > read

Над каким объектом производится операция? 1

Операция прошла успешно

Жду ваших указаний > write

Над каким объектом производится операция? 2

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 3

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 4

Какое право передается? read

Какому пользователю передается право? Ivan

Операция прошла успешно

Жду ваших указаний > quit

Работа пользователя Boris завершена. До свидания.

User:

4. Выполнить тестирование разработанной программы, продемонстрировав реализованную модель дискреционной политики безопасности.

5. Оформить отчет по лабораторной работе.

Таблица вариантов заданий

Вариант	***Количество субъектов доступа (пользователей)***	***Количество объектов доступа***
1	3	3
2	4	4
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6
11	5	3
12	6	4
13	7	4
14	8	5
15	9	6
16	10	3
17	3	4
18	4	4
19	5	5
20	6	6
21	7	3
22	8	4
23	9	4
24	10	5
25	3	6
26	4	3
27	5	4
28	6	4
29	6	5
30	8	6

Практическое занятие

Задание 1 Защита текстовых документов в Microsoft Word **.**

Задание 2. Организация защиты файлов средствами электронной таблицы MS Excel

Тема 2 «*Угрозы информационной безопасности*»:

Вопросы опроса по теме:

- Классификация угроз

- Аудит безопасности
- Каналы утечки информации
- Мероприятия по предотвращению возможных угроз на различных стадиях жизненно цикла информационных системам
- Защита от угроз информации

Примерное содержание практического занятия по теме:

Задание на лабораторную работу

1. В табл. 3 найти для указанного варианта значения характеристик *P, V, T*.

2. Вычислить по формуле (1) нижнюю границу *S** для заданных *P, V, T*.

3. Выбрать некоторый алфавит с мощностью *A* и получить минимальную длину пароля *L*, при котором выполняется условие (2).

4. Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины *L*, при этом должен использоваться алфавит из *A* символов.

5. Оформить отчет по лабораторной работе.

Коды символов:

1. Коды английских символов : «A» = 65, …, «Z» = 90, «a» = 97,…, «z» = 122.

2. Коды цифр : «0» = 48, «9» = 57.

3. «!» = 33, «“» = 34, «#» = 35, «$» = 36, «%» = 37, «&» = 38, «‘» = 39.

4. Коды русских символов : «А» – 128, … «Я» – 159, «а» – 160,…, «п» – 175, «р» – 224,…, «я» – 239.

Таблица вариантов заданий

Вариант	***P***	***V***	***T***
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
13	10^{-4}	10 паролей/день	5 дней
14	10^{-5}	20 паролей/мин	6 дней
15	10^{-6}	15 паролей/мин	12 дней
16	10^{-7}	3 паролей/мин	1 месяц
17	10^{-4}	10 паролей/мин	3 недели
18	10^{-5}	11 паролей/мин	20 дней
19	10^{-6}	100 паролей/день	15 дней
20	10^{-7}	10 паролей/день	1 неделя
21	10^{-4}	20 паролей/мин	2 недели
22	10^{-5}	15 паролей/мин	10 дней
23	10^{-6}	3 паролей/мин	5 дней
24	10^{-7}	10 паролей/мин	6 дней

Вариант	*P*	*V*	*T*
25	10^{-4}	11 паролей/мин	12 дней
26	10^{-5}	100 паролей/день	1 месяц
27	10^{-6}	10 паролей/день	3 недели
28	10^{-7}	20 паролей/мин	20 дней
29	10^{-4}	15 паролей/мин	15 дней
30	10^{-5}	3 паролей/мин	1 неделя

Тема 3: «*Вредоносные программы и противодействие им*»

Вопросы опроса по теме:

- Классификация вредоносных программ
- Особенности проявления вирусов различного вида
- Механизмы проникновения вирусов, их внедрения и распространения
- Меры ответственности за распространение вредоносных программ
- Методы и средства защиты от компьютерных вирусов
- Антивирусные программы, виды, функциональное назначение
- Использование антивирусного программного обеспечения в информационных системах
- Защита информации в системах электронной почты

Примерное содержание практического занятия по теме:

Лабораторная №3

Варианты заданий

1. Разработать консольное приложение для шифрования/дешифрования произвольных файлов с помощью алгоритма RSA.
2. Разработать визуальное приложение для шифрования/дешифрования изображений.
3. Разработать визуальное приложение для шифрования/дешифрования произвольных файлов.
4. Разработать клиент-серверное приложение для защищённой передачи файлов по сети.
5. Разработать клиент-серверное приложение для защищённого обмена сообщениями по сети.
6. Разработать визуальное приложение для шифрования/дешифрования чисел.
7. Разработать консольное приложение для генерации ключей.
8. Реализовать программу для шифрования / дешифрования текстов, работающую по алгоритму RSA. Программа должна уметь работать с текстом произвольной длины.

Лабораторная №3

Варианты заданий

1. Разработать консольное приложение для шифрования/дешифрования произвольных файлов с помощью алгоритма RSA.
2. Разработать визуальное приложение для шифрования/дешифрования изображений.
3. Разработать визуальное приложение для шифрования/дешифрования произвольных файлов.
4. Разработать клиент-серверное приложение для защищённой передачи файлов по сети.
5. Разработать клиент-серверное приложение для защищённого обмена сообщениями по сети.
6. Разработать визуальное приложение для шифрования/дешифрования чисел.
7. Разработать консольное приложение для генерации ключей.
8. Реализовать программу для шифрования / дешифрования текстов, работающую по алгоритму RSA. Программа должна уметь работать с текстом произвольной длины.

Тема 4 «Методы и средства защиты компьютерной информации»:
Вопросы опроса по теме:

- Средства идентификации и аутентификации
- Управление доступом к ресурсам ИС
- Аудит безопасности
- Механизмы проникновения вирусов, их внедрения и распространения
- Меры ответственности за распространение вредоносных программ.
- Системы управления отслеживания активности сотрудников предприятия как средство защиты от внутренних угроз.

Примерное содержание практического занятия по теме:

Лабораторная работа №4 Разработка антивирусных программ

Цель занятия: Получить практический опыт по разработке антивирусной программы.

Задание на лабораторную работу:

1. Разработать простейшую программу- вирус.
2. Разработать антивирусную программу для данного вируса.

Тема 5 «Криптографические методы информационной безопасности»:
Вопросы опроса по теме:

- Что представляет собой криптосистема?
- Как определяется криптостойкость?
- В чём разница между симметричными и ассиметричными криптографическими системами?
- Какие основные способы применяются при создании алгоритмов симметричных криптосистем?
- Какими свойствами должен обладать абсолютно стойкий шифр?
- Каковы основные характеристики алгоритма DES?
- Каковы основные характеристики алгоритма криптографического преобразования по ГОСТ 28147-89?
- Что лежит в основе ассиметричной криптографии?
- В чём особенности и основные сферы применения ассиметричных криптосистем?

Примерное содержание практического занятия по теме:
Лабораторная работа №5 Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра

Задание на лабораторную работу

Разработать программу, реализующую привязку к компьютеру, используя совокупность характеристик согласно варианту задания. Добиться того, чтобы программа не запускалась на другом компьютере.

Таблица вариантов заданий

№ варианта	Характеристики
1	Серийный номер раздела жесткого диска, MAC-адрес сетевой карты
2	Информация из реестра, тактовая частота процессора
3	Версия операционной системы, MAC-адрес сетевой карты
4	Имя пользователя, серийный номер раздела жесткого диска
5	Название компьютера, информация из реестра
6	Версия БИОС, имя пользователя
7	Серийный номер раздела жесткого диска, имя пользователя
8	Имя пользователя, тактовая частота процессора
9	MAC-адрес сетевой карты, тактовая частота процессора

Тема 6 «Лицензирование и сертификация в области защиты информации»:

Вопросы опроса по теме:

- Какие НПА регулируют правоотношения в сфере лицензирования и сертификации в РФ?
- Какие виды деятельности в сфере защиты информации подлежат лицензированию?
- Каков механизм получения лицензии и какие органы осуществляют лицензирование?
- В чем заключается процедура сертификации?
- Как осуществляется обязательная и добровольная сертификация?
- Государственная система и практика обеспечения информационной безопасности.

Примерное содержание практического занятия по теме:

Практическое занятие № 6 Выбор СКУД по техническим показателям

Задание

Ответить на вопросы:

- что обеспечивается с применением технических средств?
- на какие системы могут быть разделены технические средства охраны по своему функциональному назначению?
- для чего предназначены технические системы охранной сигнализации?
- Оборудование охраняемого объекта техническими средствами охраны.
- Аргументировать выбор технических средств охраны

Тема 7 «Критерии информационной безопасности, оценки рисков и управление её обеспечением»:

Вопросы опроса по теме:

- Содержание «Оранжевой книги»
- Базовые требования безопасности
- Критерии безопасности
- Основные концепции безопасности и ход развития средств защиты.
- Основные понятия международного стандарта ISO/IEC 15408.
- Критерии безопасности в руководящих документах Гостехкомиссии и ФСТЭК РФ
- Назначение и деятельность структуры ГОССОПКА
- Назначение, использование и управление DLP-системами в организация мониторинга компьютерной активности сотрудников

Примерное содержание практического занятия по теме:

Практическая работа №7 Система конфиденциальной информации фирмы

Порядок выполнения занятия

Работа выполняется в форме деловой игры.

Суть игры заключается в том, что начальник организации (преподаватель) ставит общую задачу: разработать комплекс мер, направленных на защиту коммерческой тайны. Ресурсы не ограничиваются.

Учебная группа разделяется на несколько рабочих коллективов.

В каждом коллективе студенты самостоятельно выбирают модератора (руководитель отдела по защите информации). Модератор распределяет задание для выработки мер защиты коммерческой тайны по схеме классификации защитных действий среди сотрудников своего отдела (студентов).

По готовности модераторы докладывают о выборе мер.

Преподаватель уточняет защитные действия у ответственных лиц (студентов группы, отвечающих за данное направление).

После заслушивания всех модераторов преподаватель комментирует работу каждой группы, даёт общее заключение, проводит работу над ошибками.

Письменный отчёт по работе не представляется. Все записи о предлагаемых мерах студентами фиксируются в конспектах.

Практическая работа №8 Составление плана мероприятий по защите информации при подготовке к проведению совещания

Задание

Разработать план проведения конфиденциального совещания.

Практическая работа №9 Успешность реализации политики безопасности

Задание

Создать план мероприятий по обеспечению комплексной безопасности обучающихся в институте.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Зачет с оценкой проводится с применением следующих методов (средств): проведение зачета с оценкой, включающего теоретическую часть и практико-ориентированное задание, требующее демонстрации уровня владения умениями/навыками.

5.2. Оценочные материалы промежуточной аттестации

Таблица 4.

Показатели и критерии оценивания

Компонент компетенции	Промежуточный индикатор оценивания	Критерий оценивания
ОПК-3.2 Способен применять различные поисковые системы, электронные библиотеки и базы знаний при решении задач профессиональной деятельности	ИОПК-3.2 Применяет различные поисковые системы, электронные библиотеки и базы знаний при решении задач профессиональной деятельности	На основе поиска российских и зарубежных аналитических центров, а также журналов в области программной инженерии принимать решение о об использовании современных программных средств в области CASE-технологий, их настройке и использовании с учётом выполнения условий их поставки и лицензирования.
ОПК-4.2 Способен принимать участие в разработке технической документации на различных этапах жизненного цикла информационной системы в рамках совместного группового	ИОПК-4.2 Принимает участие в разработке технической документации на различных этапах жизненного цикла информационной системы в рамках совместного группового	Разрабатывает техническую документацию на различных этапах жизненного цикла информационной системы в рамках совместного группового проекта, связанного с

Компонент компетенции	Промежуточный индикатор оценивания	Критерий оценивания
проекта, связанного с профессиональной деятельностью	проекта, связанного с профессиональной деятельностью	профессиональной деятельностью

Перечень теоретических вопросов к зачёту

1. Комплексный подход к обеспечению информационной безопасности.
2. Основные понятия защиты информации.
3. Угрозы информационной безопасности и каналы утечки информации.
4. Организационно-правовое обеспечение информационной безопасности.
5. РД «Классификация автоматизированных систем и требования по защите информации» Гостехкомиссии России и характеристика девяти классов защищённости.
6. ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
7. Профиль защиты. Функциональные требования и требования доверия.
8. Каталог функций безопасности объекта.
9. Предположения безопасности и сокращение избыточных требований.
10. Понятие политики безопасности и ролевое управление информационной безопасностью.
11. Аппаратные и программные методы защиты данных.
12. Типы несанкционированного доступа к компьютерным системам и условия работы средств защиты.
13. Защита от локального несанкционированного доступа.
14. Защита от удалённого несанкционированного доступа.
15. Защита от несанкционированного доступа к информации в коммутируемых каналах связи.
16. Методы восстановления информации.
17. Обобщённый класс программ - разрушающие программные воздействия.
18. Модели взаимодействия прикладной программы и программной и программной закладки.
19. Методы перехвата и навязывания информации.
20. Классификация и методы внедрения программных закладок.
21. Компьютерные вирусы как особый класс разрушающих программных воздействий.
22. Защита от разрушающих программных воздействий. Изолированная программная среда.
23. Проблема защиты алгоритма, возникающая при проектировании и реализации системы защиты информации.
24. Способы встраивания защитных механизмов в программное обеспечение.
25. Симметричные и ассиметричные криптосистемы.
26. Способы создания симметричных криптосистем. Абсолютно стойкий шифр.
27. Криптографическая система DES и её модификации.
28. Алгоритм криптографического преобразования по ГОСТ 28147-89.
29. Принципы построения ассиметричных криптографических систем.
30. Назначение и использование электронной цифровой подписи.
31. Хеширование и ГОСТ Р 34.11-94.
32. Современные алгоритмы электронной цифровой подписи и ГОСТ Р 34.10-94.
33. Проблема подмены открытого ключа.
34. Комплексный метод защиты информации.
35. Методы защиты межсетевого обмена данными.
36. Аппаратные шифраторы. Структура. Техническая реализация.

37. Программный продукт PGP.
38. Взаимодействие брандмауэров и систем обнаружения вторжений.
39. Государственная политика РФ в области информационной безопасности.
40. Структура органов ГосСОПКА и их место в деле обеспечения информационной безопасности Российской Федерации.

Перечень практико-ориентированных (практических) заданий к зачету

ОПК-3.2 - способен применять различные поисковые системы, электронные библиотеки и базы знаний при решении задач профессиональной деятельности:

1. В сети Интернет найти информацию о вирусных опасностях для компьютеров, антивирусных программах. На основе найденной информации составить их рейтинг и особенности использования.
2. Группе студентов найти программу шифрации сообщений для мобильной связи, установить их на свои телефоны и продемонстрировать её использование при взаимной связи. Описать алгоритм работы такой программы.

ОПК-4.2 - способен принимать участие в разработке технической документации на различных этапах жизненного цикла информационной системы в рамках совместного группового проекта, связанного с профессиональной деятельностью:

1.Для указанной предметной области и структурно организованного уровня предприятия разработать политику безопасности.
2. Представить структурную схему процессов управления информационной безопасностью предприятия с указанием входных данных и выходных результатов.

Шкала оценивания

Промежуточная аттестация проводится в форме зачета (дифференцированного зачета - зачет с оценкой) без применения балльно-рейтинговой системы оценивания - посредством аттестационных испытаний в форме традиционного зачета.

Результаты промежуточной аттестации оцениваются: экзамена - по традиционной балльной системе оценивания («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»); зачета — по бинарной системе оценивания («зачтено», «не зачтено»), или традиционной балльной системе оценивания.

Наряду с оцениванием учебных достижений обучающихся по принятой образовательной организации системе оценок и использованием ее при оформлении официальных дипломов Академии о высшем образовании, вводят повышенный («Excellent» и «Good») и базовый («Very good» и «Satisfactory») уровень оценок «отлично» и «хорошо» для использования при оформлении ЕПД, согласно Положению об оформлении и выдаче ЕПД.

Таблица 5.

Соответствие академической оценке

Академическая оценка		Оценка по шкале ESTS	
зачтено	отлично	Passed	A (Excellent)
			B (Very Good)
	хорошо		C (Good)
			D (Satisfactory)
	удовлетворительно		E (Sufficient)
не зачтено	неудовлетворительно	-	-

Критерии оценивания в ходе промежуточной аттестации

Оценка **«отлично»** выставляется обучающемуся:

– если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно излагает его на экзамене, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими

видами знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение; учебные достижения и результаты текущего контроля успеваемости демонстрируют высокую степень сформированности соответствующих компетенций.

Оценка **«хорошо»** выставляется обучающемуся:

– если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения; учебные достижения и результаты текущего контроля успеваемости демонстрируют хорошую степень сформированности соответствующих компетенций.

Оценка **«удовлетворительно»** выставляется обучающемуся:

– если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ; учебные достижения и результаты текущего контроля успеваемости демонстрируют удовлетворительную степень сформированности соответствующих компетенций.

Оценка **«неудовлетворительно»** выставляется обучающемуся:

если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы; учебные достижения и результатами текущего контроля успеваемости демонстрируют низкую степень сформированности соответствующих компетенций.

6. Методические материалы по освоению дисциплины с применением ЭК

Обучение по дисциплине «Информационная безопасность» предполагает изучение курса на аудиторных занятиях (лекции, практические) и самостоятельной работы студентов. Практические занятия дисциплины «Алгоритмы сортировки, поиска и сжатия данных» предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций.

Подготовка к лекции студентами заключается в следующем:

– повторить материал предыдущей лекции, прочитав его повторно;

– ознакомиться с темой предстоящей лекции (в рабочей программе учебной дисциплины);

– ознакомиться с учебными материалами по данной теме в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины или с электронными материалами, предложенными лектором;

– записать возможные вопросы, которые можно будет задать лектору.

Подготовка к практическим (семинарским) занятиям:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы, предложенные в рабочей программе дисциплины для обсуждения;

– выполнить задания, если они предусмотрены в письменной форме;

– понять, что для вас осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическим/семинарским занятиям можно как индивидуально, так и в составе малой группы;

– рабочую программу учебной дисциплины необходимо использовать в качестве основного ориентира в организации обучения;

– электронная версия рабочей программы по дисциплине размещена на сайте Нижегородского института управления, к ней предоставлен авторизованный доступ.

Самостоятельная работа обучающегося:

Самостоятельная работа призвана закрепить теоретические знания и практические навыки, полученные на лекциях, практических и семинарских занятиях.

Самостоятельная работа проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений обучающихся;
- углубления и расширения теоретических знаний;
- формирования умений использовать справочную документацию и специальную литературу;
- развития познавательных способностей и активности: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Эффективность лекционных, семинарских и практических занятий по дисциплине во многом зависит от качества самостоятельной работы обучающихся, от их самоподготовки.

Часть времени, отведенного на самостоятельную работу должна использоваться на подготовку к аудиторным занятиям, другая часть на выполнение домашней работы, осмысление и оформление результатов практических занятий.

При подготовке к занятиям студенту полезно:

- изучить теоретический материал по данной теме (конспект занятия);
- ознакомиться с литературой, рекомендованной преподавателем;
- выполнить задания, предложенные преподавателем, к занятию;
- составить перечень вопросов, вызывающих затруднения, неясности или сомнения, обсудить их с преподавателем или на занятии;
- заниматься самостоятельным поиском дополнительной литературы по изучаемой теме.

Подготовка к зачету. К зачету необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:

– программой дисциплины;

– перечнем знаний и умений, которыми студент должен владеть;

– тематическими планами лекций, семинарских занятий;

– учебником, учебными пособиями по дисциплине, а также электронными ресурсами;

– перечнем и тематикой письменных работ, а также методическими рекомендациями по их выполнению;

– перечнем вопросов.

Систематическое выполнение всех видов заданий на лекциях, практических занятиях, а также самостоятельная работа позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета.

Вопросы для самостоятельной подготовки к занятиям

1. Что понимается под политикой безопасности в компьютерной системе?

2. В чем заключается модель дискреционной политики безопасности в компьютерной системе?

3. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?

4. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту компьютерной системы?

5. Чем определяется стойкость подсистемы идентификации и аутентификации?

6. Перечислить минимальные требования к выбору пароля.

7. Перечислить минимальные требования к подсистеме парольной аутентификации.

8. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?

9. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

10. Дайте определение алгоритма с открытым ключом.

11. Сколько этапов содержит алгоритм RSA?

12. В чем заключается вычисление ключей алгоритма RSA?

13. Как происходит шифрование в алгоритме RSA?

14. Как происходит дешифрование в алгоритме RSA

15. Что понимается под «привязкой» к компьютеру?

16. Какие характеристики обычно используются для идентификации компьютера?

17. Перечислите основные API-функции для определения индивидуальных характеристик компьютера.

18. Что представляет собой реестр Windows?

19. Какую структуру имеет реестр?

20. Дайте определение и опишите основные характеристики политики безопасности.

21. Обоснуйте важность основных положений раздела «Рабочее место». Какие дополнительные требования необходимо ввести для Вашей организации?

22. Опишите как бы Вы ввели процедуру официального получения разрешения на доступ к ресурсам?

23. Составьте список возможностей Вашей организации, реализуемых с помощью сети Интернет. Каких доработок в связи с особенностями работы компании требует раздел «Работа в сети Интернет»?

24. Необходима ли разработка и внедрение политики безопасности в рассматриваемые на практических занятиях организации? Обоснуйте свой ответ.

25. Дайте определение понятию «Биометрические ПДн», опишите особенности этой категории ПДн.

26. Укажите законные основания, на основе которых Ваша организация обязана обрабатывать персональные данные.

27. Составьте список угроз безопасности ПДн при их обработке в Вашей компании.

28. Продумайте и составьте правила учета машинных носителей ПДн в Вашей организации.

29. Продумайте и составьте правила обеспечения безопасности обработки ПДн сотрудников организации.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1 Основная литература

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2024. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536902 (дата обращения: 25.04.2024). — Режим доступа: для авторизир. пользователей

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537000 (дата обращения: 25.04.2024). — Режим доступа: для авторизир. пользователей.

3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029 (дата обращения: 25.04.2024). — Режим доступа: для авторизир. пользователей.

7.2 Дополнительная литература

1. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 269 с. - ISBN 978-5-9765-1256-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843184 (дата обращения: 18.03.2024). – Режим доступа: по подписке.

2. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1898839 (дата обращения: 18.03.2024). – Режим доступа: по подписке.

3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290 (дата обращения: 25.04.2024). – Режим доступа: по подписке.

4. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2022. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490026 (дата обращения: 25.04.2024). – Режим доступа: по подписке.

7.3 Учебно-методическое обеспечение самостоятельной работы.

1. Электронные информационно-образовательные ресурсы Нижегородского института управления – филиала РАНХиГС - http://sdo.niu.ranepa.ru/
2. http://isec.ru/ - сайт Информационная безопасность
3. http://fstec.ru/ - сайт ФСТЭК РФ
4. http://www.securitylab.ru/ - информационный портал в области защиты информации
5. Электронные информационно-образовательные ресурсы Нижегородского института управления – филиала РАНХиГС - http://sdo.niu.ranepa.ru/

7.4 Нормативные правовые документы.

1. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации"
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями)
3. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями и дополнениями)
4. Приказ Министерства образования и науки РФ от 05.04.2017 №301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»
5. Образовательный стандарт ФГБОУ ВО «Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации», утвержденный приказом ректора Академии от 07.09.2023 № 01-24607 и разработанного на основе федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 №922 (зарегистрировано в Министерстве юстиции Российской Федерации 12.10.2017, регистрационный номер № 48531) и приказа Минобрнауки России от 26 ноября 2020 г. № 1456 «О внесении изменений в федеральные государственные образовательные стандарты высшего образования» (зарегистрировано в Минюсте России 27.05.2021 г., регистрационный № 63650).
6. Конституция Российской Федерации с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ)
7. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001. № 195-ФЗ (ред. 02.06.2016 N 161-ФЗ)
8. Гражданский кодекс Российской Федерации. Часть четвертая от18.12.2006 Редакция от 28.11.2015(с изм. и доп.
9. Трудовой Кодекс Российской Федерации об от 30.12.2001. № 197-ФЗ
10. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ
11. Федеральный закон «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания» от 14.06.94 г. № 5-ФЗ // Собрание законодательства Российской Федерации. 1994. № 8. Ст. 801.
12. Федеральный закон «О рекламе» от 18.07.95 г. № 108-ФЗ // от 21.07.2005 N 113-ФЗ)
13. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.95 г. № 144-ФЗ Редакция от 29.06.2015
14. Федеральный закон «Об электронной цифровой подписи» от 10.01.02 г. №1-ФЗ
15. Федеральный Закон от 27.07. 2006 . № 149–ФЗ «Об информации, информационных технологиях и о защите информации» Редакция от 13.07.2015
16. Федеральный Закон от 27.07. 2006 . № 152–ФЗ «О персональных данных» Редакция от 21.07.2014
17. Федеральный закон РФ «О средствах массовой информации» от 27.12. 1991 № 2124-1
18. Федеральный закон РФ «О государственной тайне» от 21.07.93 г.
19. Постановление Правительства Российской Федерации «О государственном учете и регистрации баз и банков данных»
20. Указ Президента РФ от 06.10.2004 N 1286 "Вопросы Межведомственной комиссии по защите государственной тайны

21. Указ Президента РФ «СТРАТЕГИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ» от 31.12.2015г. №683

22. Указ Президента Российской Федерации «О перечне сведений, отнесенных к государственной тайне» от 30.11.95 г. №1203;

23. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. М., 1990.

24. ГОСТ 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования и методы испытания. М.: Изд-во Стандартов, 1999.

25. ГОСТ 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М., 2000.

26. ГОСТ Р 50922-96. Защита информации: Основные термины и определения. М., 1996.

27. ГОСТ Р-22.0.04-95. Безопасность в чрезвычайных ситуациях. Биолого-социальные чрезвычайные ситуации. Термины и определения. М., 1995.

28. «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021).

29. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)» (утв. приказом ФСТЭК России от 02.06.2020 N 76).

30. Постановление Правительства РФ от 15.10.2021 N 1754 „Об утверждении требований к проверке простой электронной подписи, которой в соответствии с частями 5 и 23 статьи 14.1 Федерального закона “Об информации, информационных технологиях и о защите информации» подписаны согласия на обработку персональных данных и биометрических персональных данных, при хранении указанных согласий" [КОДЕКС]

31. Постановление Правительства РФ от 21.02.2022 N 222 «Об утверждении Правил представления заинтересованным лицам документа о полномочиях физического лица в случае, предусмотренном частью 2 статьи 17.1 Федерального закона „Об электронной подписи“

32. Приказ Минцифры России от 27.08.2021 N 896 «Об утверждении требований к деловой репутации единоличного исполнительного органа или членов коллегиального исполнительного органа организации, владеющей информационной системой, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающей услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц» (Зарегистрировано в Минюсте России 17.09.2021 N 65045).

33. Приказ ФСБ России от 28.09.2021 N 379 «Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранным государством, его государственными органами, международной или иностранной организацией, иностранными гражданами или лицами без гражданства могут быть использованы против безопасности Российской Федерации».

34. Приказ Министра обороны РФ от 17.01.2022 N 22 «Об утверждении Перечня сведений Вооруженных Сил Российской Федерации, подлежащих отнесению к служебной тайне в области обороны» (Зарегистрировано в Минюсте России 28.02.2022 N 67528)

35. Постановление Правительства РФ от 02.09.2021 N 1472 «Об определении информационных систем, включенных в инфраструктуру, обеспечивающую информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, с использованием которых осуществляется информационное взаимодействие федерального органа исполнительной власти, уполномоченного Правительством Российской Федерации на

осуществление государственного кадастрового учета, государственной регистрации прав, ведение Единого государственного реестра недвижимости и предоставление сведений, содержащихся в Едином государственном реестре недвижимости, и депозитария, осуществляющего хранение электронной закладной или обездвиженной документарной закладной, и о внесении изменения в Положение об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме».

7.5. Интернет-ресурсы

1. Портал Информационные технологии в образовании http://www.ict.edu.ru/
2. Федеральный портал Российское образование http://www.edu.ru/ ,
3. Единое окно доступа к информационным ресурсам http://window.edu.ru/resource/514/44514 .
4. Портал Национального Университета Открытого Образования «ИНТУИТ» https://eduopenru.ru/

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

8.1. Материально-техническая база

Перечень материально-технического обеспечения:

1. Учебные аудитории, оборудованные для проведения учебных занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, коллоквиумов, мероприятий текущего контроля и промежуточной аттестации, в том числе мультимедийным оборудованием для демонстрации электронных презентаций и аудио- и видеоматериалов.
2. Компьютерные классы для выполнения групповых тестовых и иных заданий, а также для самостоятельной работы обучающихся оснащенные компьютерной техникой и обеспечением доступа к сети «Интернет» и доступа в электронную информационно-образовательную среду организации.
3. Специализированные аудитории и лаборатории.
4. Библиотека с обеспечением печатными изданиями или электронно-библиотечная система обеспечивающая доступ к электронным изданиям (электронная библиотека).
5. Читальный зал.
6. Технические средства обучения: персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV и др.

8.2. Информационные технологии, программное обеспечение:

При осуществлении образовательного процесса по дисциплине используется информационные технологии и программное обеспечение:

1. Современная операционная система.
2. Kaspersky Endpoint Security (или аналог).
3. Средство просмотра файлов формата pdf.
4. Современные офисные средства (текстовые и табличные редакторы, средства работы с презентационными материалами и т.д.).
5. Архиватор 7-Zip.
6. Система дистанционного обучения.
7. Автоматизированная библиотечная система.

8. СУБД PostgreSQL.
9. Lucidchart.
10. Eclipse
11. Система ADVANTA для управления проектами.
12. Lucidchart.
13. Eclipse
14. LanAgent Standard 4x.
15. Lan2 Net Firewall 4x.
16. LanAgent Terminal 4x

8.3. Информационные справочные системы:

1. https://www.urait.ru –Электронно-библиотечная система [ЭБС] Юрайт;
2. http://www.iprbookshop.ru – Электронно-библиотечная система [ЭБС] «IPR SMART» (ранее – IPRBooks)
3. https://e.lanbook.com - Электронно-библиотечная система [ЭБС] «Лань».
4. https://znanium.com - Электронно-библиотечная система [ЭБС] «Znanium.com».
5. https://www.book.ru - Электронно-библиотечная система [ЭБС] «Book.ru».
6. https://ibooks.ru - Электронно-библиотечная система [ЭБС] «ibooks.ru».
7. https://www.ezproxy.ranepa.ru:2443/login?url=https://dlib.eastview.com/ – East View. Полные тексты российских научных и практических журналов, а так же газет центральной прессы России.
8. https://www.ezproxy.ranepa.ru:2443/login?url=https://grebennikon.ru/ - Полные тексты 38 научно-практических журналов по маркетингу, менеджменту, финансам и управлению персоналом ИД «Гребенников»
9. http://www.consultant.ru/ - Справочно-правовая система «Консультант».
10. http://www.garant.ru/ Справочно-правовая система «Гарант».