

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

---

**ИНСТИТУТ ОТРАСЛЕВОГО МЕНЕДЖМЕНТА  
Факультет инженерного менеджмента  
Кафедра теории и систем отраслевого управления**

УТВЕРЖДЕНА

кафедрой теории и систем отраслевого  
управления

Протокол от «28» августа 2019 г.

№ 1

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Б1.Б.05 Информационная безопасность**

---

направление подготовки

27.03.05 – Инноватика

направленность (профиль) "Технологическое предпринимательство"

Квалификация

Бакалавр

Форма обучения

Очная

Год набора - 2020

Москва, 2019 г.

**Автор–составитель:**

Преподаватель кафедры теории и систем отраслевого управления Н.И. Пышков

Заведующий кафедрой теории и систем отраслевого управления, к.э.н., доцент С.С. Серебренников

## **СОДЕРЖАНИЕ**

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся и место дисциплины в структуре образовательной программы
3. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий и структура дисциплины
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине
5. Методические указания для обучающихся по освоению дисциплины
6. Основная и дополнительная учебная литература, необходимая для освоения дисциплины, ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине
7. Материально-техническая база, информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

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

1.1. Дисциплина Б1.Б.05 «Информационная безопасность» обеспечивает овладение следующей компетенцией с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-1	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-1.1	Способность оценивать уровень развития информационной и библиографической культуры и содействовать обеспечению информационной безопасности

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Код этапа освоения компетенции	Результаты обучения
ОПК-1.1	<p><b>на уровне знаний:</b></p> <p>содержания основных понятий в области информационной безопасности;</p> <p>требований к организации процесса обеспечения защиты информации;</p> <p>методов и средств обеспечения информационной безопасности;</p> <p>методов нарушения конфиденциальности, целостности и доступности информации;</p> <p>правового обеспечения информационной безопасности в РФ и международном сообществе;</p> <p>основ безопасности операционных систем и компьютерных сетей;</p> <p>основных технических и программно-аппаратных средств защиты информации</p> <p><b>на уровне умений:</b></p> <p>обеспечивать процесс управления системой информационной безопасности компании;</p> <p>обнаруживать и оценивать слабые стороны существующей системы защиты информации;</p> <p>оперативно решать возникающие проблемы информационной безопасности в процессе непрерывного функционирования организации;</p> <p>проводить анализ угроз нарушения информационной безопасности;</p> <p>оценивать уровень развития культуры информационной безопасности;</p>

	<p>использовать отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем</p> <p><b>на уровне навыков:</b></p> <p>выполнения полного объема работ, связанных с комплексным обеспечением информационной безопасности на основе изученных программ и методик;</p> <p>обеспечения требований стандартов и нормативных документов, регламентирующих обеспечение информационной безопасности;</p> <p>обеспечения процесса принятия управленческого решения по обеспечению защиты информации;</p> <p>выполнения оперативного управления деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик</p>
--	---

**2. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся и место дисциплины в структуре образовательной программы**

#### Объем дисциплины

Вид учебных занятий и самостоятельная работа		Объем дисциплины, час.	
		Всего	Семестр
			3
Очная форма обучения			
Контактная работа обучающихся с преподавателем, в том числе:		32	32
лекционного типа (Л)		16	16
лабораторные работы (практикумы) (ЛР)			
практического (семинарского) типа (ПЗ)		16	16
Самостоятельная работа обучающихся (СР)		76	76
Промежуточная аттестация	форма	зачет	зачет
	час.		
Общая трудоемкость (час. / з.е.)		108/3	108/3

#### Место дисциплины в структуре ОП ВО

Дисциплина Б1.Б.05 «Информационная безопасность» изучается в 3 семестре по очной форме обучения, общая трудоемкость дисциплины – 3 зачетные единицы, 108 часов.

Дисциплина реализуется после изучения дисциплины Б1.Б.04 «Информационные технологии».

Форма промежуточной аттестации – зачет.

**3. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий и структура дисциплины**

**Структура дисциплины**

№ п/п	Наименование тем	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Очная форма обучения								
Тема 1	Информационная безопасность: предмет и содержание	12	2		2		8	ДИ, К
Тема 2	Технологии в сфере информационной безопасности	14	2		2		10	О, КР
Тема 3	Планирование системы информационной безопасности	12	2		2		8	О, РЗ
Тема 4	Управление рисками в сфере информационной безопасности	14	2		2		10	ДИ, К
Тема 5	Руководства и стандарты в сфере информационной безопасности	14	2		2		10	О, К
Тема 6	Правовое обеспечение информационной безопасности: зарубежная и российская практика	14	2		2		10	О, К
Тема 7	Нарушения и ответственность в сфере информационной безопасности	14	2		2		10	ДИ, РЗ
Тема 8	Культура информационной безопасности	14	2		2		10	ДИ, КР
Промежуточная аттестация								За
Всего:		108	16		16		76	

Примечание:

\* – формы текущего контроля успеваемости: опрос (О), кейс (К), дискуссия (ДИ), контрольная работа (КР), решение задач (РЗ);

\*\* - форма промежуточной аттестации: зачет (За).

**Содержание дисциплины**

**Тема 1. Информационная безопасность: предмет и содержание**

Предмет и задачи теории информационной безопасности. Базовые термины и определения. Объекты защиты и объекты моделирования. Угрозы безопасности: разновидности и классификация. Принципы информационной безопасности. Триада CIA.

Процесс обеспечения защиты информации. Надежность системы безопасности: параметры, характеристики и требования. Уязвимости в защите информационных систем. Системы информационный защиты организации. Политика информационной безопасности. Защита от несанкционированного доступа: идентификация, аутентификация, управление доступом.

## **Тема 2. Технологии в сфере информационной безопасности**

Уязвимости вычислительного оборудования. Методы и средства защиты информации. Криптографическая защита. Числовое программное управление. Управление разработкой ПО. Управление средствами ПО. Аппаратное управление. Программное управление

Модели безопасности: регламенты и критерии определения безопасности. Дискретные модели. Модель Харрисона-Рузо-Ульмана. Модель Белла ЛаПадула. Модель информационных потоков Грэхэма-Деннинга. Модель Биба. Модель Кларка-Уилсона. Модель «Китайской стены».

Криптография. Криптографический анализ: основы. Перестановка, транспозиция и диаграммы. Шифр Виженера. Стандарты DES. Алгоритмы IDEA, CAST и AES. Криптографическая система с открытым ключом. Аутентификация отправителя, Алгоритм RSA. Тенденции развития криптографической защиты. Квантовое шифрование. Блокчейн шифрование. Применение блокчейн-технологий.

Сетевая безопасность. Компьютерные сети: основные понятия. LAN, WAN, DNS-сервер и MAC-адрес. Протоколы TCP/UDP/IP. Сетевая модель OSI. Протоколы IPv4 и IPv6. Протокол UDP. Промежуточное ПО. Технологии VPN и Proxu. Системы IDS, IPS и SEIMs. Разновидности сетевых атак. Тенденции развития сетевой безопасности. Гипервизор. Виртуализация сервисов. Микросегментация сетей. Защищенные облачные вычисления. Модели SaaS, PaaS и IaaS.

## **Тема 3. Планирование системы информационной безопасности**

Процесс планирования безопасности: основные этапы и принципы. Понятие системы информационной безопасности в организации. Основополагающие методы и абстрактные модели контроля доступа. Модели и методы ролевого и сессионного контроля доступа. Вопросы идентификации ролей и сессий. Задачи построения системы защиты информации. Уровни стратегии безопасности. Классы организационных решений в информационной безопасности. Альтернативные методы защиты информации.

Проектирование систем информационной безопасности. Служба информационной безопасности. Определение функциональных задач системы защиты информации. Определение требований к качеству разработки и технического сопровождения системы защиты информации. Экономическое обоснование проектных решений. Оценка производительности системы защиты информации. Эксплуатационное проектирование системы защиты информации. Служба информационной безопасности.

## **Тема 4. Управление рисками в сфере информационной безопасности**

Управление рисками. Модель безопасности с полным перекрытием. Управление информационной безопасностью. Методики построения систем защиты информации. Методики и программные продукты для оценки рисков. Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель».

Оценка рисков организации в сфере информационной безопасности. Снижение риска: методы. Анализ и экспертиза рисков. Оценка затрат и рисков. Модель для оценки стоимости программного обеспечения COBRA. Модель процесса управления рисками.

## **Тема 5. Руководства и стандарты в сфере информационной безопасности**

Процесс построения и оценки систем информационной безопасности. Роль стандартов в безопасности информационных систем. Программное обеспечение для улучшения процессов. Стандарты ISO/IEC 17799/27002 и 27001. Модель SSE-CMM: ключевые конструкции и концепции. Архитектура SSE-CMM. Стандарты «Радужная

серия». Общие критерии оценки защищённости информационных технологий (Common Criteria). Критерий оценки безопасности информационных технологий ITSEC. Гармонизация международных и российских стандартов.

#### **Тема 6. Правовое обеспечение информационной безопасности: зарубежная и российская практика.**

Зарубежная нормативно-правовая база в сфере информационной безопасности. Акт о компьютерном мошенничестве и злоупотреблении (CFAA). Закон о защите компьютерной информации (CSA). Закон об ответственности и переносе данных о страховании здоровья граждан (HIPAA). Закон Сарбейнса-Оксли (SOX). Федеральный закон об управлении информационной безопасностью (FISMA). Общий регламент по защите данных (GDPR).

Ограничение доступа к информации в целях защиты интересов личности, общества и государства. Правовые режимы тайн в системе организационного и правового обеспечения безопасности информации ограниченного доступа. Правовой режим защиты государственной тайны. Правовой режим коммерческой тайны. Правовой режим обеспечения безопасности персональных данных. Актуальные вопросы режима служебной тайны. Противодействие экстремистской деятельности в информационной сфере. Защита детей от информации, причиняющей вред их здоровью и развитию. Правовые проблемы обеспечения информационной безопасности в сети Интернет.

#### **Тема 7. Нарушения и ответственность в сфере информационной безопасности**

Понятие и виды юридической ответственности в области обеспечения информационной безопасности. Субъекты и объекты правоотношений в области обеспечения информационной безопасности. Компьютерная криминалистика: основные положения. Типы и область преступлений. Проблема отсутствия единого юридического пространства в сфере информационной безопасности: «за» и «против». Сбор доказательств в судебном порядке. Комплаенс в сфере информационной безопасности. Формальная процедура сбора данных. Юридические основы соблюдения формальности процедуры и изъятие доказательств. Актуальные проблемы и угрозы мировой информационной безопасности.

#### **Тема 8. Культура информационной безопасности**

Информационное общество. Глобальные проблемы информатизации общества. Информационно-психологическая безопасность и манипулирование. Поведенческие аспекты безопасности информационных систем. Угрозы для сотрудников. Индивидуальная мотивация для предотвращения кибератак. Киберпреступность: преступники и средства массовой информации. Кибершпионаж и отслеживание.

Культура и информационная система безопасности. Понимание концепции культуры безопасности. Лидерство и культура безопасности. Принципы ОЭСР по культуре безопасности. Этические и профессиональные проблемы в управлении безопасностью ИС.

### **4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации дисциплине**

#### **4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации**

##### **4.1.1. В ходе реализации дисциплины используются следующие методы текущего контроля успеваемости обучающихся:**

- при проведении занятий лекционного типа:  
опрос, дискуссия;
- при проведении занятий семинарского типа:



контрольная работа, кейс;

- при контроле результатов самостоятельной работы студентов:  
решение задач.

#### **4.1.2. Зачет проводится в письменной и устной форме решением кейса и ответом на вопросы билета**

#### **4.2. Материалы текущего контроля успеваемости обучающихся**

##### **Типовые оценочные материалы по теме 1**

###### **Вопросы к дискуссии**

1. Несмотря на то, что безопасности информационных систем касается далеко не только технической оснащенности, но и правовых, организационных и прочих аспектов, ресурсы организации могут быть защищены исключительно с помощью новейших технологий безопасности. Разве данное утверждение не противоречит само себе?

2. Появление межсетевых организаций и возросшая зависимость компаний от Интернета для ведения бизнеса только увеличивает вероятность нарушений безопасности. Так ли это? Обсудите эту проблему, используя примеры из популярной прессы.

3. Действительно ли нам нужно придавать большое значение неформальному контролю до введения четких норм и требований до обеспечения безопасности? Почему «да» и почему «нет»? Аргументируйте свой ответ.

4. Чрезмерный контроль над управленческим решением и бюрократизация формальной части информационной безопасности усложняет систему и имеет негативные последствия для целостности каждой операции. Прокомментируйте данное утверждение.

###### **Решение кейса**

Кейс: Виртуальные компании и кража персональных данных

Американская авиакомпания JetBlue – это виртуальная компания, которая стала растущим трендом в гиперконкурентной глобальной экономике. Тем не менее, JetBlue не раз подвергалась хакерским атакам на протяжении 2008 – 2011 годов. Украдена информация более чем о 160 миллионах кредитных карт, что само по себе не является необычным. Однако в связи с уникальной структурой компании и размытой ответственностью за произошедшее, атака подчеркивает серьезное нарушение ответственности между клиентами и JetBlue. Атака началась с установки вредоносного ПО на устаревшие компьютерные системы, которые должны были быть заменены в скором времени. После расследования об утечке были уведомлены лишь сотрудники компании, а также местные судебные органы власти. Пассажиры и общественность не были уведомлены о каких-либо проблемах, и в конечном итоге общественности было предоставлено лишь ограниченное сообщение, в котором было подтверждено, что персоналу JetBlue был предоставлен кредитный мониторинг в течение одного года бесплатно.

Чем эта атака отличается от других по всему миру? Единственным разумное объяснение – это то что JetBlue является виртуальной компанией и частным коммерческим предприятием, конкурирующим за тех же внутренних и международных клиентов. Однако, аналогичные зарубежные авиакомпании получают субсидии или принадлежат стране, в которой находится. В этой связи, на JetBlue ложится много накладных расходов, которые не ограничиваются только ценами на топливо, рабочей силой, дорогими основными средствами и потребностью в высококвалифицированном персонале. Следовательно, чтобы сократить расходы и в то же время обеспечить высокое качество обслуживания клиентов с быстрым бронированием, простотой доступа и низкой ценой, JetBlue настойчиво устранял фиксированные расходы, такие как централизованные центры обработки вызовов, которые напрямую не связаны с поиском самолетов. Поэтому вместо

кол-центров агенты работают из дома, а задачи администрирования автоматизированы или предоставляются удаленно из компьютерных центров.

Цель состоит в 100% времени безотказной работы, это означает не только географическое распределение рабочей силы, но и их взаимосвязь с надежными телекоммуникациями и услугами. Это может объяснить, почему старые системы уязвимы для взлома, так как они находились в постоянном использовании.

Корпоративная культура теперь вступает в игру с дизайном виртуальной компании. Здесь используется следующая логика: если у компании практически нет физического контакта между работником и работодателем, как в случае с агентами в JetBlue, то персонал и клиентская база становятся абстракцией для менеджмента, устраняя благосостояние сотрудника и клиента как ощутимая реальность для менеджмента. Тогда возникает вопрос, может ли виртуальная компания обеспечить реальную заботу и заботу о своих сотрудниках и клиентах?

От действий JetBlue в этом случае нужно было бы сказать «нет», поскольку JetBlue отреагировал не на то, чтобы немедленно информировать клиентскую базу, а только позже, чтобы предоставить элементарные кредитные проверки для затронутого персонала. Как тогда противодействовать такой ситуации, поскольку виртуальные компании благодаря своей гибкости и экономии затрат будут продолжать расти и формировать будущий деловой мир? Предлагаемое решение состоит не в том, чтобы вернуться к корпоративным структурам 19 или 20 века, а в том, чтобы зафиксировать потерю информации о клиентах или сотрудниках из-за ошибки, пренебрежения или плохого дизайна как естественного аспекта бизнеса. Используемый пример будет для потери личной информации, но это может также быть расширено на другие области, такие как кредитная и медицинская информация.

Предлагаемое решение - это система самовосстановления, которая обнаруживает и устраняет попытку нарушения, но видима в общении с клиентами, властями и персоналом, затронутых нарушением. Возвращаясь к случаю JetBlue в момент обнаружения и подтверждения того, что произошло нарушение, автоматизированные процедуры перейдут в действие. В этом случае формируются цифровые сертификаты, которые будут выдаваться для всех пользователей системы. Публичные уведомления и участие правительства будут инициироваться посредством заранее определенных меморандумов о взаимопонимании, чтобы обеспечить полное осознание нарушения. В то же время сервера будут автоматически сканироваться и проверяться с кратким списком оборудования с истекшим сроком эксплуатации, которое будет заменено по ускоренному графику.

1. Какая цель внедрения подобных систем самовосстановления?
2. Какие шаги нужно предпринять для обеспечения безопасности и целостности виртуальных компаний?

## **Типовые оценочные материалы по теме 2**

### **Вопросы к опросу**

1. На техническом уровне существует шесть угроз аппаратному, программному обеспечению и данным, которые находятся в компьютерных системах. Назовите их.
2. Каких три критических требования безопасности выделяют для защиты данных?
3. Для чего использование принципа доступа к информации в пределах, необходимых для непосредственного выполнения должностных обязанностей, является наиболее приемлемой формой обеспечения?
4. Какое требование гарантирует, что данные и программы будут изменены авторизованным пользователем?
5. Какая отрасль науки стремится обеспечить конфиденциальность передаваемых сообщений, поддерживать их целостность и доступность для нужных людей в нужное время?

6. Как называется совокупность методов, используемых для взлома зашифрованных сообщений, называется
7. Как называется документ после шифрования?
8. Назовите шифры, которые используют один и тот же ключ для шифрования и дешифрования открытого текста?
9. Опишите первую линию защиты частной информации и запрет доступа злоумышленникам к защищенной системе во внутренней сети?
10. Какая методика выполняет две функции: скрывает внутренние IP-адреса критически важных систем, а также предоставляет доступ нескольким хостам в частной внутренней локальной сети выходить в Интернет, используя один публичный IP-адрес?

### **Контрольная работа**

1. Перечислите основные пройденные методы шифрования. Нарисуйте концептуальную карту того, как их можно использовать в контексте розничной торговли. Возможные розничные магазины, которые можно было бы использовать: книжный, гипермаркет, продуктовый магазин.
2. Коммерческие банки обычно публикуют свою политику конфиденциальности. Найдите любую политику конфиденциальности и оцените ее с точки зрения основных концепций информационных систем.
3. Представьте, что ваш компьютер заражен рекламным ПО, и вы находитесь в виртуализованной сети. Вы систематически выполняете шаги по удалению рекламного ПО, но теперь другие серверы показывают те же баннеры, что и у вас. Опишите, что может быть не так, и какие дальнейшие шаги вы можете предпринять, чтобы обеспечить полную очистку от вредоносного ПО.

### **Типовые оценочные материалы по теме 3**

#### **Вопросы к опросу**

1. По каким причинам обычно возникают проблемы с информационной безопасностью организации?
2. Опишите структуру управления информационной безопасностью в организации.
3. От чего зависит эффективность политики безопасности?
4. При каких действиях сотрудника организации система замков и ключей становится неактуальной?
5. Какие организационные трудности не способна решить политика безопасности?
6. На каком уровне стратегии безопасности определяются ключевые решения, касающиеся инвестиций, продажи, диверсификации и интеграции вычислительных ресурсов в соответствии с другими бизнес-целями?
7. На каком уровне стратегия безопасности рассматривает угрозы безопасности и анализирует слабые стороны системы?
8. На чем следует делать акцент при разработке системы безопасности?
9. К чему может привести передача управления и ответственности системы информационной безопасности на операционный уровень организации?
10. Какой вопрос может стать критическим при разработке системы ИБ различными подразделениями организации?

#### **Решение задач**

Задача 1. Выберите корпоративную политику любой компании на ваше усмотрение. Сравните корпоративную политику с политикой безопасности. Прокомментируйте расхождения, если таковые имеются. Предложите, как можно согласовать корпоративную политику и политику безопасности.

Задача 2. Назовите наиболее известные примеры, когда произошло нарушение безопасности из-за несоблюдения политики безопасности. Провести исследование, чтобы

найти причины, по которым политика не сработала, хотя и все положения были соблюдены. Свяжите свои выводы с принципами планирования безопасности ИБ.

Задача 3. Хакеры взломали компьютер в Калифорнийском университете в Беркли и получили 1,4 миллиона имен, номеров социального страхования, адресов и дат рождения, которые использовались в рамках исследовательского проекта. Сотрудники службы безопасности проводили обычную проверку обнаружения вторжений, когда они заметили, что неавторизованный пользователь пытается получить доступ к компьютеру. Была использована база данных с известным недостатком безопасности, и было доступно исправление, которое предотвратило бы атаку. Халатность при рассмотрении известного недостатка в безопасности, по-видимому, является распространенной ошибкой среди высших учебных заведений в штате. Известно, что банки, правительственные учреждения и школы являются главными целями для хакеров. Одной из проблем в университетах может быть отсутствие подотчетности или общего департамента, который уполномочен контролировать всю систему безопасности.

А. Назовите политики и процедуры, которые позволят университетам ограничивать уязвимости, в то же время предоставляя студентам доступ к системам.

В. В конечном счете, кто должен нести ответственность за обеспечение адекватной политики безопасности?

С. Кто в вашей высшем учебном учреждении отвечает за поддержание политики безопасности и как часто она обновляется?

#### **Типовые оценочные материалы по теме 4**

##### **Вопросы к дискуссии**

1. Какая доминирующая установка определяет процесс управления рисками в обеспечении общей безопасности предприятия? Приведите примеры.

2. Если организация должна сделать управление рисками центральным в своей стратегии безопасности, каковы будут позитивные и негативные аспекты, связанные с таким решением?

3. Риск-менеджмент действительно способствует обеспечению актуальной информации о полном спектре рисков для организации. Прокомментируйте высказывание и приведите примеры организаций, следующих данной установке.

##### **Решение кейса**

Кейс: Роль инсайдеров при нарушении системы безопасности

В апреле 2005 года была раскрыта мошенническая схема, предназначенная для кражи приблизительно 220 миллионов фунтов стерлингов у Mitsui Bank в Лондоне. Утверждалось, что члены команды уборщиков разместили аппаратные устройства на клавиатурных портах нескольких компьютеров банка для регистрации записей клавиатуры. Следователи обнаружили несколько устройств, все еще подключенных к задней панели компьютеров. Группа также стерла или остановила запись системы видеонаблюдения, чтобы скрыть следы. Полиция в Израиле задержала члена банды уборщиков для допроса после того, как он попытался перевести 23 млн фунтов стерлингов на свой банковский счет. Предполагается, что подозреваемый является младшим членом банды, а остальные остаются на свободе. По словам представителя лондонского отдела по борьбе с киберпреступностью, преступники не смогли перевести какие-либо средства, поэтому пока деньги не потеряны. Внемание отдела экспертизы теперь сосредоточено на устройствах регистрации ключей, которые были вставлены в порты клавиатуры USB. Устройства можно приобрести в нескольких шпионских магазинах в Интернете и использовать для загрузки паролей или других данных, используемых для аутентификации пользователей в защищенных системах. Беспроводные клавиатуры также представляют собой угрозу, и считается, что с тех пор банк запретил их использование. По данным аудиторов программного обеспечения Centennial Software, подавляющее большинство опрошенных ИТ-менеджеров не предприняли никаких действий, чтобы предотвратить попадание таких

устройств на рабочее место, хотя многие из них признали, что USB-устройства хранения данных представляют угрозу. «Внешние риски безопасности тщательно документированы, но теперь компании должны учитывать внутренние угрозы, которые потенциально могут нанести еще больший ущерб», - сказал Энди Бертон, исполнительный директор Centennial Software.

Доступное программное обеспечение, которое может снизить этот риск, но также должны быть введены политики, ограничивающие доступ к чувствительным компьютерам. Портативные USB-устройства и логгеры - это лишь некоторые из высокотехнологичных методов, которые преступники используют для использования слабых мест компьютера. Компьютерные преступники становятся все более изощренными, так как организованные преступные группировки обнаружили, что киберпреступность предлагает большие выгоды и меньший риск.

В 2014 году в калифорнийской школе Corona del Mar были исключены 11 учеников, когда было обнаружено, что частный репетитор велел ученикам менять свои оценки на компьютере учителя. Ученики использовали регистратор ключей в качестве средства для получения доступа. Частный репетитор, Тимоти Лай, был замешан, и была обнаружена огромная полоса фальсификации оценок. Интересно, что аппаратные регистраторы ключей являются законными, и было несколько случаев, когда сообщалось о случаях «регистрации внутренних ключей», когда члены семьи использовали такие устройства, чтобы шпионить друг за другом.

1. В чем может быть причина того, что многие ИТ-менеджеры игнорируют угрозу со стороны портативных USB-устройств?

2. Какие меры могут быть приняты для ограничения внутренних угроз, таких как Mitsui Bank?

3. Должны ли устройства регистрации ключей быть законными? Что может быть полезным для устройств регистрации ключей?

## **Типовые оценочные материалы по теме 5**

### **Вопросы к опросу**

1. Назовите четыре типа доступа, которые могут быть в базе данных CRUD, а также представляют четыре типа нарушений безопасности, которые могут возникнуть в системах?

2. Какие процедуры контроля должны регистрировать состояние системы, а затем проверять, и исправлять неисправности?

3. По какой причине ежегодно происходит рост киберпреступлений, не смотря на концентрацию мер безопасности на предотвращении преднамеренных нарушений?

4. Назовите средства управления программой, устраняющие неисправности в системе ИБ?

5. Что пытается определить аудит системы информационной безопасности в случае сбоя системы?

6. Как называется средство управления, которое используется на этапах анализа и проектирования жизненного цикла систем в качестве инструмента для понимания и регламентирования других контрольных точек в системе?

7. Каким принципам должен отвечать грамотный контроль системы ИБ?

8. Назовите модель, используемую для оценки аспектов безопасности целевой организации?

9. Как называется процесс создания инфраструктуры и корпоративной культуры, которая устанавливает методы, практики и процедуры?

10. Что необходимо учесть в системе ИБ в течение всего жизненного цикла предприятия?

### **Решение задач**

Задача 1. Придумайте компанию-разработчик программного обеспечения для критически важных приложений. Разработать меры для оценки уровня зрелости для каждого из уровней SSE-CMM. Предложите причины, по которым ваши меры должны быть приняты.

Задача 2. Составьте список всех возможных стандартов безопасности, которые вы можете найти. Попробуйте и охватите хотя бы стандарты в Европе и Северной Америке. Классифицируйте стандарты в соответствии с жизненным циклом разработки систем и прокомментируйте полезность каждого из стандартов.

Задача 3. Ревизия системного контроля Департамента внутренней безопасности для удаленного доступа выявила несколько недостатков, которые подвергают DHS риску злонамеренных хакерских атак. «Ревизия, проводимая Офисом Генерального инспектора, предписана новыми правилами FISMA, которые затрагивают федеральные агентства. В отчете было выявлено несколько конкретных недостатков: (1) узлы удаленного доступа не обеспечивают надежную защиту от несанкционированного доступа; (2) системы не были соответствующим образом исправлены; и (3) модемы, которые могут быть неавторизованы, были обнаружены в сетях DHS. В отчете говорится, что «из-за этих воздействий удаленного доступа возрастает риск того, что посторонние люди могут получить доступ к сетям DHS и поставить под угрозу конфиденциальность, целостность и доступность конфиденциальных информационных систем и ресурсов». Прокомментируйте достоинства каждого или сделайте свои рекомендации.

## **Типовые оценочные материалы по теме 6**

### **Вопросы к опросу**

1. Какие основные законы в области защиты информации в РФ, ЕС и США?
2. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности.
3. Что такое концепция информационной безопасности?
4. Что такое конфиденциальная информация?
5. Что такое персональные данные?
6. В каких случаях возможно использовать персональные данные без согласия обладателя? Охарактеризуйте биометрические данные как персональные данные.
7. Что такое профессиональная тайна?
8. Что такое коммерческая тайна?
9. Что такое режим коммерческой тайны?
10. Что такое государственная тайна?

### **Решение кейса**

Кейс: ФТК против корпорации Wyndham Destination

Давайте рассмотрим дело Федеральной торговой комиссии против Wyndham Worldwide Corporation, Дело связано с нарушением кибербезопасности в Уиндеме. ФТК подала в суд на компанию госпиталя и три ее дочерние компании из-за утечки данных, когда были получены миллионы долларов мошеннических платежей по потребительским кредитам и дебетовым картам.

У ФТК есть два основания, по которым она может подать гражданский иск. Одним из них является утверждение об обмане - другими словами, аргумент, что некоторые организации по обслуживанию потребителей (такие как, например, Wyndham Hotels) сделали ложные представления для потребителей. Второе основание для принудительного исполнения ФТК – это более широкое обоснование того, что компания занималась «несправедливой» деловой практикой, иными словами, что компания «нанесла или может нанести существенный ущерб потребителям, так что потребители не могут поступать рационально».

Иск утверждает два основания для юрисдикции ФТК. Сначала утверждается, что политика конфиденциальности Wyndham в отношении того, как они будут поддерживать

безопасность информации о своих клиентах, является обманчивой, иными словами, Wyndham дала обещания безопасности, которые она не сможет выполнить. В иске также утверждается, что систематическая неспособность Wyndham обеспечить адекватную кибербезопасность для личной информации своих клиентов является несправедливой деловой практикой.

Этот тип иска со стороны ФТК не является необычным. Эти правовые теории послужили, например, основой расследования ФТК Google, Twitter и HTC, а также расследования нарушений данных в крупных потребительских компаниях, таких как Heartland. Почти во всех этих случаях ФТК использует некоторую комбинацию аргумента, что компания ввела общественность в заблуждение относительно природы своей кибербезопасности («обмана») или что она не смогла адекватно инвестировать в меры кибербезопасности («недобросовестная практика»). До сих пор все эти действия приводили к внесудебным расчетам, в результате чего действительность правовых теорий ФТК не проверялась.

Усилия ФТК являются единственным эффективным аспектом федеральной программы, чтобы заставить бизнес-сообщество принять более строгие меры кибербезопасности. В то время как мнения разделились, чтобы, если последствие усилий FTC хорошо или плохо, это бесспорно, что результаты, когда компании платят правдоподобность судебного процесса увеличились. Поскольку закон о кибербезопасности еще введен, а исполнительный приказ администрации находится в стадии разработки. ФТК – последний «борец за справедливость».

Но сейчас - в случае с Wyndham - авторитет ФТК ставится под сомнение. Wyndham оспаривает основную предпосылку иска ФТК, утверждая, что законы о защите прав потребителей не могут быть расширены для охвата вопросов кибербезопасности. Wyndham утверждал, что судебный процесс превышает полномочия ФТК.

Основным доказательством того, что FTC может действовать вне его полномочий, является его собственный доклад от 2000 года, в котором он просил Конгресс расширить свои юридические полномочия, чтобы рассматривать нарушения безопасности как проблемы защиты потребителей. Конгресс никогда не действовал по этой просьбе, но ФТК решил продолжить в любом случае. Действительно, как отмечает Wyndham, в книгах уже есть целый ряд более конкретных законов о защите данных (HIPAA; COPPA; Graham-Leach-Bliley), предполагающих, что ФТК действует как орган регулирования.

Теперь мы можем понять, почему это важно. В отсутствие всеобъемлющего законодательства о кибербезопасности и в то время, как мы ожидаем разработки стандартов кибербезопасности для исполнительного распоряжения, единственным эффективным методом «государственного регулирования кибербезопасности» является использование правоохранительных органов ФТК. Если, в конце концов, окажется, что ФТК не хватает полномочий, которые он утверждает, тогда у правительства не будет никакой реальной власти, чтобы обязать компании ужесточать требования к кибербезопасности. Некоторые увидят это как победу, а другие увидят это как поражение, но в любом случае это будет весьма важно. (Примечание: в конечном итоге принято решение в пользу ФТК.)

1. Прокомментируйте аспекты полномочий и ответственности различных законодательств. Каков наилучший способ возложить ответственность за кибербезопасность на агентство и при этом иметь полномочия на его выполнение?

2. В таких ситуациях, как с ФТК, какие правила следует разрабатывать, чтобы контролировать последующие действия в случаях кибербезопасности?

3. По мере развития технологии, что следует делать, чтобы организации соблюдали законодательство?

## **Типовые оценочные материалы по теме 7**

### **Вопросы к дискуссии**

1. Право собственности на Передача компьютера третьему лицу (например, для

ремонта) может привести к потере конфиденциальности. Как можно решить эту проблему с точки зрения нарушения конфиденциальности?

2. «Информация, представленная в Системе обнаружения вторжений, полезна для борьбы с компьютерными преступлениями». Прокомментируйте юридическую допустимость такой информации.

3. Сегодня руководители служб безопасности выполняют сложную задачу по обеспечению правопорядка в информационном пространстве. Учитывая, что безопасность действительно является сложной, межатраслевой задачей, прокомментируйте роль компьютерной криминалистики в общей безопасности предприятия.

### **Решение задач**

Задача 1. Найдите несколько примеров компьютерных преступлений. Соберите информацию о видах доказательств, и возникающих проблемах, если таковые имеются. Сделайте выводы и представьте лучшие практики для компьютерной криминалистики.

Задача 2. В июне 2002 года молодой хакер смог взломать серверы в секретной оружейной лаборатории в Соединенных Штатах. Осознав, что произошло нарушение безопасности; часть лабораторий была закрыта на три дня, опасаясь, что это связано с террористической атакой. Позже стало известно, что подросток просто хотел загрузить музыку и фильмы и использовал серверы лаборатории в качестве места для хранения файлов. Он разработал программное обеспечение, позволяющее ему загружать защищенные авторским правом материалы, и назвал его Deathserv. Возможно, его не поймали так быстро, если бы он не рассказал друзьям о своей схеме, и именно он и его друзья увеличили трафик на сервере, что предупредило власти. Подросток получил легкий приговор, частично из-за его возраста. Судья Эндрю Гоймер в лондонском королевском суде Саутворка приговорил Макелроя к 200 часам общественных работ после признания себя виновным в несанкционированном изменении содержимого компьютера. Министерство энергетики США потребовало компенсацию в размере 21 000 фунтов стерлингов в связи с серьезностью преступления и возмещением убытков в результате нарушения работы сети и расследования.

1. Какой вывод следует сделать молодым нарушителям?
2. Поможет ли международный набор правил вынесения приговоров в таких ситуациях, учитывая безграничный характер Интернета?
3. Какие инструменты расследования могли быть использованы для отслеживания хакера и выяснения его личности?

## **Типовые оценочные материалы по теме 8**

### **Вопросы к дискуссии**

1. В своем обращении к бальному залу, в котором сегодня сидят главные высшие должностные лица по вопросам информационной безопасности, Гейл Теккере, специальный юрисконсульт по технологическим преступлениям при Генеральном прокуроре штата Аризона, сказал, что ИТ-директора должны «лучше работать», защищая инфраструктуру страны, - заявил Теккерея: Если вы хотите защитить свои вещи от людей, которые не разделяют ваши ценности, вам нужно работать лучше. Вы должны сделать это в сочетании с правоохранительными органами по всей стране .... Вам нужны более эффективные способы общения с отраслью и правоохранительными органами. Будет только хуже». Прокомментируйте данное высказывание?

2. Люди, которые склонны представлять наибольшую угрозу безопасности – это люди, которые имеют низкую самооценку и сильно желают одобрения своих сверстников. Люди, которые уделяют больше внимания ассоциациям и дружбе в отношении поддержания системы ценностей организации, могут нанести серьезный ущерб безопасности. Прокомментируйте.

3. Упражнение.

4. Какие страны лидируют в сфере стандартизации риск-менеджмента?



5. Что такое COSO?
6. Существует ли единый, обязательный для всех стран стандарт управления рисками фирмы, работающей на международном рынке?

#### **Контрольная работа**

1. Провести исследование, чтобы выяснить, как культура безопасности развивается и поддерживается в средах, не основанных на ИТ. Как можно извлечь уроки из этих реализаций для развития и поддержания культуры безопасности ИС?

2. Представьте, что вы недавно получили диплом бакалавра в области информационных систем. Хотя вы проходили несколько курсов по кибербезопасности в своем бакалавриате, у вас нет практической подготовки по данному предмету. Нарисуйте путь для себя, чтобы вы были успешным специалистом по безопасности. Какие дополнительные курсы вы должны пройти? На каких сертификатах стоит сосредоточиться? Какой путь вы видите в своей карьере на следующий день?

3. Представьте, что сотрудник вашей компании нарушает установленную политику безопасности, в частности, посещая нежелательные веб-сайты, совершая покупки в Интернете во время работы и так далее. Какие внутренние и внешние факторы мотивации вы бы определили, чтобы сотрудник придерживался правил политики безопасности?

### **4.3. Оценочные средства для промежуточной аттестации**

#### **4.3.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы**

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-1	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-1.1	Способность оценивать уровень развития информационной и библиографической культуры и содействовать обеспечению информационной безопасности

#### **4.3.2. Показатели и критерии оценивания компетенций на различных этапах их формирования**

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ОПК-1.1	оценивает уровень развития информационной и библиографической культуры; оценивает уровень вовлеченности заинтересованных сторон в	<b>на уровне знаний:</b> содержания основных понятий в области информационной безопасности; требований к организации процесса обеспечения защиты информации;

	<p>процесс обеспечения информационной безопасности</p>	<p>методов и средств обеспечения информационной безопасности;</p> <p>методов нарушения конфиденциальности, целостности и доступности информации;</p> <p>правового обеспечения информационной безопасности в РФ и международном сообществе;</p> <p>основ безопасности операционных систем и компьютерных сетей;</p> <p>основных технических и программно-аппаратных средств защиты информации</p> <p><b>на уровне умений:</b></p> <p>обеспечивать процесс управления системой информационной безопасности компании;</p> <p>обнаруживать и оценивать слабые стороны существующей системы защиты информации;</p> <p>оперативно решать возникающие проблемы информационной безопасности в процессе непрерывного функционирования организации;</p> <p>проводить анализ угроз нарушения информационной безопасности;</p> <p>оценивать уровень развития культуры информационной безопасности;</p> <p>использовать отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем</p> <p><b>на уровне навыков:</b></p> <p>выполнения полного объема работ, связанных с комплексным обеспечением информационной безопасности на основе изученных программ и методик;</p> <p>обеспечения требований стандартов и нормативных документов, регламентирующих обеспечение информационной безопасности;</p> <p>обеспечения процесса принятия управленческого решения по обеспечению защиты информации;</p> <p>выполнения оперативного управления деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных</p>
--	--	--

		систем на основе разработанных программ и методик
--	--	---

### **4.3.3. Типовые контрольные задания или иные материалы (типичные оценочные материалы), необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

#### **Типовые варианты билетов**

##### **Билет №1**

Кейс: Кибератака на Playstation Network.

В мае 2011 года корпорация Sony подверглась кибератаке, которое затронуло 25 миллионов клиентов. Атака была совершена через Playstation Network. Злоумышленники из-за пределов США смогли проникнуть в сеть Sony Playstation Network и «освободить» 23 400 финансовых записей за 2007 год. Кроме того, были похищены подробные банковские записи 10 700 клиентов из Германии, Испании, Австрии и Нидерландов. Sony сообщила, что имена, адреса, электронные письма, даты рождения, номера телефонов и другая неопознанная информация были украдены с устаревшего сервера базы данных. Физическим местом атаки был дата-центр Sony в Сан-Диего. Это была вторая атака за неделю, и Sony не могла понять, как она могла пережить вторую атаку за такой короткий период. Во время первой атаки утверждалось, что кибер-злоумышленники украли информацию более чем 77 миллионов пользователей Playstation.

Компания Sony была атакована преступной хакерской организацией LulzSec. Идея взлома состоит в том, чтобы заставить приложение непреднамеренно запускать код SQL. Если приложение по незнанию создает строки SQL на лету, а затем выполняет эти строки, возникают некоторые интересные результаты. Предполагая, что хакер LulzSec имел некоторые предварительные знания о приложении и доступе к исходному коду, у него было бы представление о том, насколько универсальным будет SQL-сервер для такой крупной корпорации, как Sony (Unixwiz). Microsoft SQL Server стала системой управления базами данных (СУБД) для предприятий, которым требуется гибкий набор функций по более низкой цене, чем другие СУБД. В любой крупной корпорации можно с уверенностью предположить, что СУБД SQL Server находится в фоновой базе данных. Если потенциальный хакер заинтересован в обнаружении базы данных SQL, все, что ей нужно сделать, это покопаться в системе. Во время просмотра Веб-страницы корпорации, проверьте страницу входа в систему для традиционной формы username-and-password, а также ссылку для отправки мне по электронной почте. Это может оказаться вредным и привести к краху всей системы. При вводе адреса электронной почты система предполагает поиск адреса электронной почты в базе данных пользователей и отвечает, отправляя что-либо по этому адресу. Так как адрес электронной почты не найден, он не может ничего отправлять. Проблема с сетью Sony в том, что у них не была настроена защита от SQL-инъекций для предотвращения второй атаки. Атаки SQL-внедрения используют вредоносный код, вставленный в строки, которые затем передаются экземпляру SQL Server для анализа и выполнения. Любые процедуры, которым разрешено создавать операторы SQL, следует проверять на наличие уязвимостей внедрения, поскольку SQL Server не настолько умен и будет выполнять любые синтаксически допустимые запросы, которые он получает. Опытный и решительный злоумышленник может манипулировать параметризованными данными.

Новые вызовы безопасности современного бизнеса делают традиционные схемы безопасности неуместными. Многие архитектуры безопасности спроектированы с использованием правил, ориентированных на периметр, и не имеют всеобъемлющих параметров внутреннего контроля. Большинство организаций, зависящих от технологии

безопасности брандмауэра, могут раздвинуть границы и попросить механизмы безопасности сделать больше, чем было задумано. Старые наборы правил брандмауэра содержат таблицы, которые остаются неизменными годами. Это может быть известным недостатком, когда наборы правил брандмауэра не соответствуют современным требованиям бизнеса и не обеспечивают надлежащей защиты критически важных активов. Одним из первых шагов по защите сети является глубокая перестройка политики сегментации корпоративной сети. Политика реализуется для описания того, какие отделы, приложения, модель сервиса и активы должны находиться в отдельных сетях. Сегментация сети поможет обеспечить сдерживание потенциальных угроз с минимальным воздействием на корпоративную сеть. Учреждения по стандартизации, такие как Национальный институт стандартов и технологий, подчеркивают важность сегментации сети, но не соответствуют требованиям. Комитеты по стандартам подчеркивают новые руководящие принципы, согласно которым потенциал соответствия может быть значительно уменьшен путем размещения всех связанных активов в одном сегменте. Сегментация сети - это здравый смысл на современном рынке, а также одно из самых эффективных и экономичных ограничений для внедрения. Возврат инвестиций в реализацию (ROI) максимизируется с минимальными затратами.

Вопросы:

1. Как такие компании, как Sony, должны защищать свою репутацию? В частности, в последние годы у Sony была плохая пресса. После нарушения PlayStation Sony также столкнулась с нарушением после выхода фильма «Интервью» в 2015 году. Разработайте стратегию защиты репутации после нарушения.

2. Выскажите свое мнение о том, насколько хорошо Sony разрешила инцидент с кибербезопасностью. Учитывая, что нарушение Sony PlayStation действительно имело место, какие шаги по обработке инцидентов должны были быть выполнены?

3. Сравните и сопоставьте нарушение Sony с другим нарушением по вашему выбору. Прокомментируйте, как были обработаны два нарушения. Определите сходства и различия.

## Билет №2

Кейс: Проблемы целостности процессов и данных в системе планирования

С 2014 года Департамент по делам ветеранов постоянно проверяется на предмет скандала, связанного с увеличением времени ожидания пациентов и фальсификацией в больницах и клиниках по всей стране. Раненые ветераны сообщили, что не могли получать критическую помощь в течение нескольких месяцев из-за чрезмерного или неправильного планирования. Под пристальным вниманием Департамента в настоящее время обсуждается вопрос о том, внедрять ли домашнюю программную систему или приобрести готовое решение, поставляемое Epic Systems Corporation.

подразделение Департамента состоит из 16 000 сотрудников, которые на 50% являются постоянными работниками и 50% наемными работниками. После обвинений подразделение ОI&T признало, что они пытались заменить старую систему с 2000 года, но из-за пробелов в ИТ-навыках в отделе им пришлось обратить внимание на использование коммерческого продукта вместо разработки приложения. Неудачная реализация замены старой системы обошлась в 127 миллионов долларов, деньги, которые поступают от налогоплательщиков. Кроме того, широко распространено мнение о том, что способность увольнять и нанимать сотрудников в федеральном правительстве слишком негибкая, что позволяет немотивированным и неудовлетворительным.

Поскольку проблема, от которой страдает Департамент, связана не только с информационными технологиями, но и с целью достижения бизнес-целей, агентство получит выгоду от рекомендаций по стратегическому планированию информационных систем. Такое планирование поможет агентству обеспечить адекватное решение проблем, связанных с процессом и целостностью данных. Недостатки в системе планирования могут стать серьезной проблемой кибербезопасности. Это потому, что нарушенные процессы

являются средством, с помощью которого злоумышленники эксплуатируют системы. Некоторые соображения управления могут быть:

1. Технические стратегии реализации в сочетании с возвратом инвестиций агентства.
2. Индивидуальные навыки сотрудников и программы обучения наряду с организационным процессом, определяемым рабочими процессами программного обеспечения.
3. Новые методы управления проектами и гибкой разработки.
4. Новое руководство, которое создает возможности для улучшения культурных и организационных форм и устоявшихся представлений.
5. Социальная ответственность перед заинтересованными сторонами.

Перед отделом информационных технологий Департамента встала трудная задача – замены широко используемой ключевой операционной системы. Из-за критически важного характера работы больничной системы, работающей 24 часа 7 дней в неделю, они не смогут позволить себе никакого времени или задержки во время любого перехода на новую систему. Поскольку система была построена много лет назад, появились новые технологии, политики и бизнес-цели. Было бы трудно даже сделать постепенные улучшения в системе или полностью заменить систему, обеспечивая при этом удовлетворение всех потребностей нескольких больниц, больничных отделений и заинтересованных сторон. Отсутствие способности разъединять систему и постепенно улучшать меньшие порции за один раз создает огромную задачу.

Увеличение нагрузки на пациентов и ожиданий менеджмента в сочетании с минимальным финансированием и устаревшей программной инфраструктурой – все это вызвало скандал с расписанием в 2014 году. Однако с тех пор Департамент предпринял значительные усилия посредством значительных действий по реформированию для улучшения и решения этих проблем. Хотя освещение дела уже достигло кульминации в средствах массовой информации, в настоящее время все еще обсуждается, как реализовать новое решение для их задач планирования и данных системы медицинских карт. С новым руководством и поддержкой лидеров нашей страны в Конгрессе и президенте будет интересно посмотреть, сможет ли Департамент принять решение о методе реализации. Несмотря на то, что планирование и реализация проекта программного обеспечения продолжались в течение многих лет, сейчас нет лучшего времени для внедрения навыков и навыков планирования стратегических информационных систем.

#### Вопросы

1. У Департамента было несколько проблем. Некоторые были связаны с проблемами менеджмента, в то время как другие были связаны с данными и используемыми системами. Предложите, как решить каждую из проблем?
2. Выясните последствия возможных угроз безопасности, возникающих в результате «нарушенных процессов» в агентстве.
3. Если бы вас пригласили в качестве консультанта по кибербезопасности, как бы вы поступили с решением проблем?

### Шкала оценивания

Оценка	Требования к знаниям
«зачтено»	Оценка «зачтено» выставляется, если студент демонстрирует: <b>знание:</b> содержания основных понятий в области информационной безопасности; требований к организации процесса обеспечения защиты информации; методов и средств обеспечения информационной безопасности;

	<p>методов нарушения конфиденциальности, целостности и доступности информации;</p> <p>правового обеспечения информационной безопасности в РФ и международном сообществе;</p> <p>основ безопасности операционных систем и компьютерных сетей;</p> <p>основных технических и программно-аппаратных средств защиты информации</p> <p><b>умение:</b></p> <p>обеспечивать процесс управления системой информационной безопасности компании;</p> <p>обнаруживать и оценивать слабые стороны существующей системы защиты информации;</p> <p>оперативно решать возникающие проблемы информационной безопасности в процессе непрерывного функционирования организации;</p> <p>проводить анализ угроз нарушения информационной безопасности;</p> <p>оценивать уровень развития культуры информационной безопасности;</p> <p>использовать отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем</p> <p><b>навыки:</b></p> <p>выполнения полного объема работ, связанных с комплексным обеспечением информационной безопасности на основе изученных программ и методик;</p> <p>обеспечения требований стандартов и нормативных документов, регламентирующих обеспечение информационной безопасности;</p> <p>обеспечения процесса принятия управленческого решения по обеспечению защиты информации;</p> <p>выполнения оперативного управления деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик</p>
«не зачтено»	<p>Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «не зачтено» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.</p>

#### 4.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Студент должен выполнить все задания и мероприятия, предусмотренные программой дисциплины (по формам текущего контроля). В случае наличия учебной задолженности студент отрабатывает пропущенные занятия в соответствии с требованиями. Оценка студента носит комплексный характер и определяется:

- ответом на зачете;
- учебными достижениями в семестровый период.

Зачет проводится в письменной и устной форме решением кейса.

На выполнение студенту отводится 90 минут. После подготовки студент сдает преподавателю задание в устной форме в формате «защиты», т.е. аргументированного отстаивания и доказательства своего решения предложенного кейса. В свою очередь, преподаватель вправе оспаривать позицию студента, приводя собственные аргументы и задавая ряд наводящих вопросы. По итогу, согласно предложенным критериям оценки, преподаватель выставляет соответствующий балл. Студент вправе оспорить полученную оценку после зачета. Результат работы озвучивается сразу по завершению проверки работы и опроса студента. Оценка «не зачтено» проставляется только в ведомости.

Сдача зачета добавляет к набранному количеству баллов не более 20.

#### Критерии оценки

Количество баллов	Требования
20-15	Выставляется студенту, полностью освоившему материал дисциплины в соответствии с учебной программой, включая вопросы, рассматриваемые в рекомендованной программой дополнительной справочно-нормативной и научно-технической литературы, свободно владеющему основными понятиями дисциплины. Требуется полное понимание и четкость изложения ответов по предложенному вопросу и дополнительным вопросам, заданным экзаменатором.
14-10	Заслуживает студент, ответивший полностью и без ошибок на предложенные вопросы и показавший знания основных понятий дисциплины в соответствии с обязательной программой курса и рекомендованной основной литературой.
9-5	Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Речевое оформление требует поправок, коррекции.
4-0	Дан неполный ответ теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.

#### Состав балльно-рейтинговой оценки

№ контрольной точки	Виды контроля	Максимальное значение в баллах
1	Решение кейса	6
2	Контрольная работа	5
3	Решение задач	4
4	Решение кейса	6
5	Решение задач	4
6	Решение кейса	6
7	Решение задач	4
8	Контрольная работа	5
Активность на лекционных занятиях (опрос)		10
Участие в дискуссиях (каждая дискуссия оценивается в 10 баллов)		30
Сумма баллов по итогам текущего контроля		80

Результат промежуточной аттестации	20
Итого	100

### Опрос

В ходе текущей аттестации проверяется знание обучающимися основных понятий по теме, необходимых для дальнейшего освоения дисциплины. Для студента предоставляется возможность продемонстрировать знание изученного материала с использованием профессиональной лексики и терминологии.

#### Критерии оценки

Количество баллов	Требования
10-8	Отвечая на поставленные вопросы, студент продемонстрировал свободное владение основными понятиями и материалом дисциплины в соответствии с учебной программой. Требуется полное понимание и четкость изложения ответов по предложенному вопросу и дополнительным вопросам, заданным преподавателем.
7-5	Заслуживает студент, ответивший полностью и без ошибок на предложенные вопросы и показавший знания основных понятий дисциплины в соответствии с обязательной программой дисциплины. Однако студент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя.
4-2	Дан недостаточно полный, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи.
1-0	Выставляется студенту при неполном ответе или отсутствии ответа, имеющего отношение к вопросу. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения.

### Дискуссия

Метод дискуссии основан на обмене мнениями между преподавателем и студентами. Высказываемые мнения отражают собственные взгляды участников дискуссии или опираются на мнения других лиц. Цепь дискуссии – достижение определенной степени согласия ее участников относительно дискутируемого тезиса.

Дискуссия должна иметь:

- тему,
- предмет,
- наличие общих исходных позиций сторон,
- характерная манера ведения дискуссии,
- готовность участников услышать позиции и мнения других.

#### Критерии оценки

Количество баллов	Требования	Критерий
2,0	Ведение дискуссии в рамках объявленной темы; видение сути проблемы.	Видение проблемы
1,5	Отклонение от темы по причине иной трактовки сути проблемы.	
1,0	Отклонение от темы по причине отсутствия сути	



	проблемы.	
0,5	Намеренная подмена темы дискуссии по причине неспособности вести дискуссию в рамках предложенной проблемы.	
0	Перескакивание с темы на тему, отсутствие всякого понимания сути проблемы.	
2,0	Точная, четкая формулировка аргументов и контраргументов, умение отделить факты от субъективных мнений, использование примеров, подтверждающих позицию сторон.	Доказательность в отстаивании своей позиции
1,5	Допущены логические ошибки в предъявлении некоторых аргументов или контраргументов или преобладают субъективные доводы над логической аргументацией или не использованы примеры, подтверждающие позицию стороны.	
1,0	Ошибки в предъявлении аргументов и контраргументов связанные с нарушением законов логики, неумение отделить факты от субъективных мнений.	
0,5	Несоответствие аргументов и контраргументов обсуждаемой проблеме, отсутствие причинно-следственных связей между аргументами и контраргументами, преобладание только субъективных доводов в отстаивании позиции сторон.	
0	Повторное утверждение предмета спора вместо его доказательства или отсутствие фактических доказательств или приведение вместо доказательств субъективных мнений.	
2,0	Соответствие аргументов выдвинутому тезису, соответствие контраргументов высказанным аргументам.	Логичность
1,5	Соответствие аргументов выдвинутому тезису, соответствие большинства контраргументов высказанным аргументам.	
1,0	Несоответствие некоторых аргументов выдвинутому тезису или несоответствие некоторых контраргументов высказанным аргументам.	
0,5	Несоответствие большинства аргументов выдвинутому тезису, несоответствие большинства контраргументов высказанным аргументам.	
0	Отсутствие всякой связи между тезисом, аргументами и контраргументами.	
2,0	Толерантность, уважение других взглядов, отсутствие личностных нападок, отказ от стереотипов, разжигающих рознь и неприязнь.	Корректность по отношению к оппоненту
1,5	Толерантность, уважение других взглядов, отсутствие личностных нападок, но перебивание оппонентов, неумение выслушать мнение оппонента до конца.	
1,0	Проявление личностной предвзятости к некоторым	

	оппонентам, неумение выслушать мнение оппонента до конца.	
0,5 0	Отсутствие терпимости к мнениям других участников дискуссии, перебивание оппонентов. Прямое игнорирование мнения других участников дискуссии, нападки на оппонентов, препятствие в проведении дискуссии, срыв дискуссии.	
2,0  1,5  1,0  0,5  0	Отсутствие речевых и грамматических ошибок, отсутствие сленга, разговорных и просторечных оборотов. Эмоциональность и выразительность речи. Допущены разговорные или просторечные обороты при отсутствии речевых и грамматических ошибок или речи допущены речевые и грамматические ошибки при отсутствии разговорных и просторечных оборотов. Эмоциональность и выразительность речи. Допущены разговорные или просторечные обороты, речевые и грамматические ошибки или отсутствует эмоциональность и выразительность речи. Небрежное речевое поведение: наличие речевых ошибок, излишнее использование сленга, разговорных и просторечных оборотов. Монотонная (или излишне эмоциональная) речь. Качество речи препятствует пониманию высказываемой мысли.	Способ речи
10	Итого	

### Решение задач

Данная форма контроля позволяет студенту прочно усвоить пройденный материал, осознать задачу и логику выполнения упражнения. Решенная задача оценивается по следующим критериям:

- Степень и уровень выполнения задания
- Правильность и полнота результатов задачи;
- Аккуратность в оформлении работы.

#### Критерии оценки

Количество баллов	Требования
4	Работа выполнена в полном объеме с соблюдением необходимой последовательности.
3	Работа выполнена не полностью, но объем выполненной части таков, что позволяет получить правильные результаты.
2	В логическом рассуждении нет существенных ошибок, но допущены существенные ошибки. Задача выполнена в общем виде.
1	Задача выполнена частично или неверно, с большим количеством ошибок. По итогу невозможно сделать правильный вывод.
0	Задача не выполнена

### Контрольная работа

Контрольная работа проводится в аудитории под контролем преподавателя. На выполнение одного варианта работы обучающемуся отводится 90 минут. Ответы подтверждаются расчетами и дается оценка полученных результатов

#### Критерии оценки

Количество баллов	Требования
5	Работа выполнена в полном объеме. Выполнены необходимые расчеты, ошибок в расчетах нет.
4-3	Выполнены необходимые расчеты, но в некоторых из них есть ошибки. Работа выполнена не полностью, но объем выполненной части позволяет сделать необходимые выводы.
2-1	Выполнены не все необходимые расчеты, в них есть серьезные ошибки. Задания выполнены в общем виде.
0	Ответы на большинство вопросов в контрольной работе не даны или даны неверно. По итогу выполненных заданий невозможно сделать правильный вывод.

#### Решение кейса

Кейс – это описание конкретной ситуации или случая в какой-либо сфере. При решении кейса оценивают две группы навыков. Первая – навыки работы с информацией и аналитика (hard skills). Здесь смотрят, насколько соотносится поставленная задача и ответ, на структуру и логику решения. Вторая группа – навыки общения и взаимодействия (soft skills). В нее входит умение презентовать решение, грамотно отвечать на вопросы и правильно их задавать. Если кейс решался в группе, то оценивается также командная работа – на выступлении или непосредственно в процессе решения.

Критерии оценки ответов:

- Полнота ответа с использованием всей информации из описания ситуации
- Обоснованность
- Умение оперировать терминами и понятиями в сфере управления персоналом
- Использование теоретических моделей и концепций
- Представленность нескольких точек зрения на проблему
- Отсутствие фактических ошибок

#### Критерии оценки

Количество баллов	Требования
6	<ul style="list-style-type: none"> <li>• изложение материала логично, грамотно, без ошибок;</li> <li>• свободное владение профессиональной терминологией;</li> <li>• умение высказывать и обосновать свои суждения;</li> <li>• студент дает четкий, полный, правильный ответ на теоретические вопросы;</li> <li>• студент организует связь теории с практикой.</li> </ul>
5-4	<ul style="list-style-type: none"> <li>• студент грамотно излагает материал: ориентируется в материале, владеет профессиональной терминологией, осознанно применяет теоретические знания для решения кейса, но содержание и форма ответа тлеют отдельные неточности;</li> <li>• ответ правильный, полный, с незначительными неточностями или недостаточно полный.</li> </ul>
3-2	<ul style="list-style-type: none"> <li>• студент излагает материал неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения кейса, не может доказательно обосновать свои суждения;</li> <li>• обнаруживается недостаточно глубокое понимание изученного</li> </ul>

	материала.
1-0	<ul style="list-style-type: none"> <li>отсутствуют необходимые теоретические знания: допущены ошибки в определении понятий, искажен их смысл, не решен кейс;</li> <li>в ответе студента проявляется незнание основного материала учебной программы, допускаются грубые ошибки в изложении, не может применять знания для решения кейса.</li> </ul>

## 5. Методические указания для обучающихся по освоению дисциплины

Процесс обучения включает следующие основные виды занятий:

1. лекции;
2. практические занятия;
3. самостоятельная работа.

На лекциях студенты изучают основные теоретические концепции риск-менеджмента, основы регулирования и стандартизации в сфере управления рисками, знакомятся с наиболее известными работами ученых и существующими практическими разработками в данной области, закрепляя полученные знания на практических занятиях. С целью обеспечения успешного обучения студенту необходимо готовиться к каждой лекции, т.к. она является важнейшей формой организации учебного процесса, поскольку знакомит с новым учебным материалом, разъясняет учебные элементы, трудные для понимания, систематизирует учебный материал, ориентирует в учебном процессе.

Подготовку к лекции рекомендуется проводить по следующему плану:

1. внимательно прочитайте материал предыдущей лекции;
2. узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);
3. ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
4. постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;
5. запишите возможные вопросы, которые вы зададите лектору на лекции

Подготовку к практическому занятию рекомендуется проводить по следующему плану:

1. внимательно прочитайте материал лекций, относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
2. выпишите основные термины;
3. законспектируйте главы из основных источников литературы, соответствующие изучаемой теме;
4. уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до семинарского занятия) во время текущих консультаций преподавателя;
5. готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы.

Получение углубленных знаний по изучаемой дисциплине достигается за счет дополнения часов аудиторной нагрузки самостоятельной работой студентов, которая выражается в анализе дополнительной литературы по учебной дисциплине по отдельным темам учебной программы.

### Подготовка к промежуточной аттестации

На первом занятии преподаватель информирует обучающихся о применяемой системе текущего контроля успеваемости и форме промежуточной аттестации.

Во время последующих аудиторных занятий – доводит до студентов информацию о результатах текущего контроля успеваемости.

К промежуточной аттестации необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессии, как правило, показывают не удовлетворительные результаты. В самом начале изучения учебной дисциплины познакомьтесь со следующей учебно-методической документацией:

1. программой дисциплины;
2. перечнем знаний и умений, которыми студент должен владеть;
3. тематическими планами лекций, семинарских занятий;
4. контрольными мероприятиями;
5. учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
6. типовым вариантом задания к промежуточной аттестации.

После этого у вас должно сформироваться четкое представление об объеме и характере получаемых знаний и умений по дисциплине. Систематическое выполнение учебной работы на лекциях и практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для прохождения промежуточной аттестации.

**Вопросы для самостоятельной подготовки к занятиям лекционного, практического (семинарского) типов**

№	Наименование тем и/или разделов	Вопросы, выносимые на самостоятельное изучение
Тема 1	Информационная безопасность: предмет и содержание	1. Ролевая модель безопасности 2. Процесс оценки и обеспечения безопасности Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата, глава 1
Тема 2	Технологии в сфере информационной безопасности	1. Ассиметричные шифры 2. Хэш-функции 3. Тренды криптографии Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата, глава 2
Тема 3	Планирование системы информационной безопасности	1. Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении 2. Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства 3. Практика разработки и реализации политики информационной безопасности корпоративных информационных систем Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, глава 6
Тема 4	Управление рисками в сфере информационной безопасности	1. Методики построения систем защиты информации 2. Методики и программные продукты для оценки рисков 3. Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель» Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата, глава 2
Тема 5	Руководства и стандарты в сфере	1. Другие различные стандарты и руководства

	информационной безопасности	Information Security. Text and Cases. Edition 2.0   Copyright 2018   Publication Date: December 2017 Gurpreet Dhillon, chapter 7
Тема 6	Правовое обеспечение информационной безопасности: зарубежная и российская практика	1. Противодействие экстремистской деятельности в информационной сфере 2. Защита детей от информации, причиняющей вред их здоровью и развитию 3. Правовые проблемы обеспечения информационной безопасности в сети Интернет Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, глава 5
Тема 7	Нарушения и ответственность в сфере информационной безопасности	1. Преступность в информационной сфере как угроза информационной безопасности при формировании информационного общества в условиях глобализации 2. Проблемы уголовно-правовой ответственности за информационные преступления 3. Проблемы международного сотрудничества и зарубежный опыт противодействия преступлениям в информационной сфере Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, глава 7
Тема 8	Культура информационной безопасности	1. Информационно-психологическая безопасность 2. Технологии манипулирования 3. Способы защиты личности 4. Информационная культура и сетевой этикет 5. Психологические особенности Интернет-общения Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов, глава 4

**6. Основная и дополнительная учебная литература, необходимая для освоения дисциплины, ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

### **6.1. Основная литература**

1. 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: <http://www.biblio-online.ru.ezproxy.ranepa.ru:3561/bcode/434171>

2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <http://www.biblio-online.ru.ezproxy.ranepa.ru:3561/bcode/450371>

3. Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <http://www.biblio-online.ru.ezproxy.ranepa.ru:3561/bcode/454453>

## **6.2. Дополнительная литература**

1. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. — Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 с. — 978-5-9963-0237-6. — Режим доступа: <http://www.iprbookshop.ru/52182.html>
2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — 978-5-94774-821-5. — Режим доступа: <http://www.iprbookshop.ru/52209.html>
3. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 268 с. — 978-89838-487-6. — Режим доступа: <http://www.iprbookshop.ru/6991.html>
4. Чернова, Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <http://www.biblio-online.ru.ezproxy.ranepa.ru:3561/bcode/449350>

## **6.3. Учебно-методическое обеспечение самостоятельной работы**

1. Information Security. Text and Cases. Edition 2.0 | Copyright 2018 | Publication Date: December 2017 Gurpreet Dhillon, The University of North Carolina at Greensboro
2. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М.: Издательство Юрайт, 2017. — 220 с.
3. Государственная тайна и ее защита в Российской Федерации: Учебное пособие // под общ.ред. М.А. Вуса и А.В. Федорова С-Пб.2007.
4. Управление финансовыми рисками: учебник и практикум для бакалавриата и магистратуры / И. П. Хоминич [и др.]; под редакцией И. П. Хоминич, И. В. Пещанской. — Москва: Издательство Юрайт, 2019. — 345 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01019-0. — С. 38 — 88 — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/bcode/433674/p.38-88>

## **6.4. Нормативные правовые документы**

1. Стратегия развития информационного общества в Российской Федерации" (утв. Президентом РФ 07.02.2008 N Пр-212)
2. Федеральный закон «Об информации, информационных технологиях и о защите информации № 149-ФЗ от 27 июля 2006 года
3. Федеральный закон от 23.08.1996 N 127-ФЗ «О науке и государственной научно-технической политике» // СЗ РФ 26.08.1996, N 35, ст. 4137
4. Распоряжение Правительства РФ от 17.11.2008 N 1662-р «О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года» // СЗ РФ 24.11.2008, N 47, ст. 5489.
5. Указ Президента РФ от 01.11.2008 № 1576 «О Совете при Президенте Российской Федерации по развитию информационного общества в Российской Федерации»
6. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»
7. Федеральный закон от 19.12.2005 N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
8. Федеральный закон от 19.12.2005 N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»

## **6.5. Интернет-ресурсы**

1. [www.nnir.ru](http://www.nnir.ru) / - Российская национальная библиотека
2. [www.nns.ru](http://www.nns.ru) / - Национальная электронная библиотека
3. [www.rsi.ru](http://www.rsi.ru) / - Российская государственная библиотека
4. [www.biznes-karta.ru](http://www.biznes-karta.ru) / - Агентство деловой информации «Бизнес-карта»
5. [www.rbs.ru](http://www.rbs.ru) / - Информационное агентство «РосБизнесКонсалтинг»
6. [www.google.com](http://www.google.com) / - Поисковая система
7. [www.rambler.ru](http://www.rambler.ru) / - Поисковая система
8. [www.yandex.ru](http://www.yandex.ru) / - Поисковая система
9. [www.businesslearning.ru](http://www.businesslearning.ru) / - Система дистанционного бизнес образования
10. <http://www.consultant.ru/> - Консультант плюс
11. <http://www.garant.ru/> - Гарант
12. [www.economist.com/](http://www.economist.com/) - журнал The Economist
13. [www.ft.com](http://www.ft.com) / - газета The Financial Times
14. [www.forbes.com/management](http://www.forbes.com/management) / - Новости бизнеса (менеджмент)
15. [www.management.about.com](http://www.management.about.com) / - Управление и лидерство
16. [www.rbc.ru](http://www.rbc.ru) / - Деловые новости
17. [www.kommersant.ru](http://www.kommersant.ru) / - газета Коммерсантъ
18. [www.vedomosti.ru](http://www.vedomosti.ru) / - газета Ведомости

## **6.6. Иные источники**

Не используются.

## **7. Материально-техническая база, информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем**

Помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие примерным программам дисциплин, рабочим учебным программам дисциплин.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационно-образовательную среду Академии.

Академия обеспечена необходимым комплектом лицензионного и свободно распространяемого программного обеспечения: MS Windows, MS Office.

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам.