Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ
Декан факультета
факультета компьютерных технологий
(наименование факультета)
Я.Ю. Григорьев
(подпись, ФИО)
«12» 03 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Руководство и управление службой безопасности

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Анализ безопасности информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2021*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
5	*10*	*3*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зачет с оценкой	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2021

Разработчик рабочей программы:

Доцент ИБАС		Соколов А.А.
(должность, степень, ученое звание)	(подпись)	(ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС		Лошманов А.Ю.
(наименование кафедры)	(подпись)	(ФИО)

1 Общие положения

Рабочая программа дисциплины «Руководство и управление службой безопасности» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации № 1509 от 01.12.2016, и основной профессиональной образовательной программы подготовки «Анализ безопасности информационных систем» по направлению 10.05.03 "Информационная безопасность автоматизированных систем".

Практическая подготовка реализуется на основе:
Профессиональный стандарт утвержденного приказом Министерства труда и социальной защиты от 15 сентября 2016 года N 522н №843 "Специалист по защите информации в автоматизированных системах" зарегистрированного в Министерстве юстиции Российской Федерации 28 сентября 2016 года, регистрационный N 43857. Обобщенная трудовая функция: **D/02.7** Разработка проектных решений по защите информации в автоматизированных системах
D/03.7 Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

Задачи дисциплины	Формирование компетенций необходимых в управлении структурными подразделениями по защите информации в составе службы безопасности предприятия. Определение теоретических, концептуальных, методологических,организационных и технических основ обеспечения безопасностиинформации на предприятии.
Основные разделы / темы дисциплины	Раздел 1 Тема 1. Информационные отношения как объект правового регулирования. Тема 2. Компьютерная система как объект информационной безопасности Тема 3. Допуск должностных лиц и граждан к государственной тайне Раздел 2 Тема 4. Организация службы защиты информации на предприятия Тема 5. Разработка должностных инструкций для лиц, ответственных за обеспечение информационной безопасности

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Процесс изучения дисциплины «Руководство и управление службой безопасности» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	**УК-3.1** Знает основные приемы и нормы социального взаимодействия; основные понятия и методы конфликтологии, технологии межличностной и деловой коммуникации, принципы командной работы как основы организации и руководства работой команды, способы мотивации членов команды с учетом организационных возможностей и личностных особенностей членов команды	**УК-3.2** Умеет устанавливать и поддерживать контакты, обеспечивающие успешную работу в команде; разрабатывать цели команды в соответствии с целями проекта; выбирать стратегию формирования команды и определять функциональные и ролевые критерии отбора участников	**УК-3.3** Имеет навыки организации и руководства работой команды, презентации результатов собственной и командной работы
ПК-6 Способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов	**ПК-6.1** Знает способы проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов	**ПК-6.2** Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов	**ПК-6.3** Владеет навыками проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Руководство и управление службой безопасности» изучается на 5 курсе(ах) в 10 семестре(ах).

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к базовой части.

Для освоения дисциплины необходимы знания, умения, навыки и (или) опыт практической деятельности, сформированные в процессе изучения дисциплин:

- Информационная безопасность предприятия;
- Защита информации в информационных системах;

- Разработка политики информационной безопасности;
- Информационная безопасность распределенных информационных систем;
- Информационная безопасность систем распределенной обработки информации;
- Аттестация объектов информатизации;

Знания, умения и навыки, сформированные при изучении дисциплины «Руководство и управление службой безопасности», будут востребованы при изучении последующих дисциплин:

- Производственная практика (проектно-технологическая пракика), 11 семестр;
- Производственная практика (преддипломная практика);
- Подготовка к процедуре защиты и защита выпускной квалификационной работы

Дисциплина «Руководство и управление службой безопасности» частично реализуется в форме практической подготовки. Практическая подготовка организуется путем выполнения лабораторных работ.

Дисциплина «Руководство и управление службой безопасности» в рамках воспитательной работы направлена на формирование у обучающихся умения аргументировать, самостоятельно мыслить, развивает профессиональные умения, ответственности за выполнение учебно-производственных заданий, проводить мониторинг защищенности информации в автоматизированных системах и оценку рисков информационной безопасности автоматизированных систем.

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 з.е., 108 акад. час.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
Общая трудоемкость дисциплины	108
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	64
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	32
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	32
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	44
Промежуточная аттестация обучающихся – Зачет	

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Раздел 1 Тема 1. Информационные отношения как объект правового регулирования. Тема 2. Компьютерная система как объект информационной безопасности Тема 3. Допуск должностных лиц и граждан к государственной тайне	16		16	22
Раздел 2 Тема 4. Организация службы защиты информации на предприятия Тема 5. Разработка должностных инструкций для лиц, ответственных за обеспечение информационной безопасности	16		16	22
ИТОГО по дисциплине	**32**		**32**	**44**

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

Компоненты самостоятельной работы	Количество часов
Изучение теоретических разделов дисциплины	14
Подготовка к занятиям семинарского типа	15
Подготовка и оформление контрольной работы	15
	44

7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 Основная литература

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.
2. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016. - 240 с.
3. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 416 с.
4. Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с
5. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с

8.2 Дополнительная литература

1. SNatives] Implement mainline Ethereum precompiles. 2019. URL: https://github.com/hyperledger/burrow/ issues/1240 (дата обращения: 02.12.2019).
2. Brown, R. G. The Five Ingredients Of Blockchain Interoperability // Forbes, 2020. URL: https://www.forbes. com/sites/richardgendalbrown/2020/02/13/the-five-ingredients-of-block-chaininteroperability/#7d3e7ce558a1 (дата обращения 13.02.2020).
3. Buterin, V. Chain Interoperability. 2016. URL: https://www.r3.com/wp-content/uploads/2017/06/chain_ interoperability_r3.pdf (дата обращения: 14.11.2019).
4. Byzantine fault tolerance (BFT) and Crash fault tolerance (CFT) // Stack Overflow, 2019. URL: https:// stackoverflow.com/questions/56336229/byzantine-fault-tolerancebft-and-crash-fault-tolerance-cft (дата обращения: 11.11.2019).
5. Chainstack. Enterprise Blockchain Protocols: Evolution Index 2020. URL: https://chainstack.com/wp-content/ uploads/2020/01/Enterprise-Blockchain-Protocols-Evolution-Index-2020.pdf (дата обращения: 22.01.2020).
6. ECDSA: (v, r, s), what is v? // Stack Exchange, 2019. URL: https://bitcoin.stackexchange.com/ questions/38351/ecdsa-v-r-s-what-is-v (дата обращения: 09.12.2019).

7. Hash Time Locked Contracts // Bitcoin Wiki. URL: https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts (дата обращения: 04.12.2019).
8. Hyperledger Burrow. Hyperledger. 2019. URL: https://www.hyperledger.org/projects/hyperledger-burrow (дата обращения: 12.11.2019).
9. ISO/IEC 17788:2014 Information technology – Cloud computing – Overview and vocabulary. 2014. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en (дата обращения: 10.12.2019).

8.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Руководство и управление службой безопасности», предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и практических занятий.

Таблица 5 Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять ключевые слова, формулы, отмечать на полях уточняющие вопросы по теме занятия
Лабораторные занятие	Работа с автоматизированными рабочими местами.
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к практическим занятиям, изучение теоретических разделов дисциплины, подготовка к контрольной работе.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Руководство и управление службой безопасности» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление контрольной работы.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий для текущего контроля;

– выполнения и защиты контрольной работы;

8.4 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1. Электронно-библиотечная система ZNANIUM.COM – http://www. znanium.com.
2. Консультант+
3. Научная электронная библиотека Elibrary http://elibrary.ru.

8.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Сайт университета www.knastu.ru[Электронный ресурс]:. Раздел сотрудникам, документы СМК, режим доступа – свободный. Загл. с экрана
2. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

8.6 Лицензионное программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 6 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты
Microsoft® Windows Professional 7 Russian	Лицензионный сертификат № 46243844 от 09.12.2009
Open Office или аналог	Свободно-распространяемое
Операционная система Kali Linux или аналог	Свободно-распространяемое
Операционная система Ubuntu или аналог	Свободно-распространяемое
Обозреватель Google Chrome или аналог	Свободно-распространяемое

9 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные

образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

1. Методические указания при работе над конспектом лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

2. Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к лабораторным занятиям

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы необходимо стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Оформлять отчеты следует руководствуясь внутренними нормативными документами КнАГУ.

3. Методические указания для выполнения лабораторных работ и контрольной работы

Лабораторная работа №1

Тема: Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности.

Цель работы:

- закрепление теоретических знаний в области правового обеспечения информационной безопасности

- исследование терминологической базы

- закрепление знаний основного понятийного аппарата, применяемого в области защиты информации

- формирование навыка работы с нормативными документами по исследуемому вопросу

Ход исследования:

1. Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации.

2. Федеральные законы в области информации и информационной безопасности.

3. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.

4. Правовые режимы защиты информации.

5. Правовые вопросы защиты информации с использованием технических средств.

Рекомендуемая литература:

1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г.
2. Конституция Российской Федерации.
3. Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 - ФЗ "О безопасности"
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»
5. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
6. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
7. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
8. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
9. Федеральный закон РФ от 29 июля 2004 г № 98-ФЗ «О коммерческой тайне».
10. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

11. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
12. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
13. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
14. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
15. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации Решение председателя Гостехкомиссии России от 25 июля 1997 г.
16. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования Решение председателя Гостехкомиссии России от 25 июля 1997 г.
17. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России.
18. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России.
19. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России.
20. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России.
21. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России.
22. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия

Теоретическая часть:

ОСНОВЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Содержание и структура правового обеспечения

Правовое обеспечение информационной безопасности является самостоятельным комплексным направлением правового регулирования отношений в области проявления угроз объектам информационной безопасности и противодействия этим угрозам на основе норм и институтов различных отраслей права (конституционного, гражданского, административного, уголовного и информационного).

Предмет правового обеспечения информационной безопасности представляет собой совокупность общественных отношений, на которые направлено правовое воздействие в целях недопущения, выявления и пресечения проявлений угроз объектам национальных интересов в информационной сфере, а также минимизации негативных последствий проявления этих угроз.

Общественные отношения, относящиеся к данному предмету, имеют следующие основные признаки:

- *принадлежность к регулируемым правом информационным отношениям*, т.е. общественным отношениям по поводу обладания необходимой информацией, передачи части имеющейся информации другим субъектам, а также сохранения в неизвестности оставшейся части информации;

- *принадлежность к объектам информационной безопасности*, которые представляются важными руководству организаций или государственных органов для эффективного достижения целей их деятельности;

- *обусловленность проявлением угроз сохранности* основных свойств объектов информационной безопасности организаций и государственных органов.

Совокупность норм и институтов права, регулирующих эти отношения, составляет содержание правового обеспечения ин формационной безопасности и может быть разделена по объектам безопасности на правовое обеспечение безопасности информации в форме сведений, правовое обеспечение безопасности информации в форме сообщений, правовое обеспечение безопасности информационной инфраструктуры и правовое обеспечение безопасности правового статуса субъекта ин формационной сферы.

Правовое обеспечение безопасности информации в форме сведений образуется совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов:

- сведения, обладателем которых является субъект права;
- свобода мысли;
- субъективная значимость национальных культурных ценностей.

Основная угроза сведениям, обладателем которых является субъект права, заключается в искажении этих сведений посредством навязывания ложной информации. В основу правового регулирования отношений в области противодействия навязыванию ложной ин формации положен принцип выделения социально опасных действий, связанных с передачей или распространением такой информации (клевета, обман и злоупотребление доверием, заведомо ложная реклама и т.п.), и их запрета под угрозой применения к виновным лицам административной или уголовной ответственности. Нормы права, регулирующие эти отношения, входят в состав отраслей административного или уголовного права.

Основная угроза свободе мысли заключается в применении средств нарушения независимости психической деятельности мозга человека, например, таких, как скрытые вставки, скрытая реклама.

Скрытая вставка представляет собой изображение, сюжет, мелодию или текстовое сообщение, которые являются составной частью программ, фильмов или компьютерных программ, относящихся к специальным средствам массовой информации. Они воспринимаются человеком через подсознание и (или) оказывают вредное воздействие на его здоровье.

В отличие от «скрытой вставки» дефиниция «скрытая реклама» в законодательстве определяется как реклама, которая оказывает не осознаваемое потребителем воздействие, в том числе путем использования специальных видеовставок (двойной звукозаписи) и иными способами.

Основу правовой конструкции регулирования отношений в рассматриваемых областях составляют нормы конституционного права, гарантирующие каждому человеку осуществление права на свободу мысли, а также нормы, предусматривающие возможность использования для защиты этого права целой системы юридических институтов, включающей институты конституционного контроля, судебной защиты, административно-правовой защиты, государственного надзора, международного контроля и международной судебной защиты. Кроме того, в состав этой конструкции входят правовые нормы, закрепляющие конституционное право человека и гражданина на охрану здоровья и медицинскую помощь, в частности на восстановление психического здоровья человека, а также нормы, регулирующие отношения в области оказания ему необходимой медицинской помощи.

Основная угроза субъективной значимости национальных культурных ценностей заключается в их девальвации вследствие пропаганды образцов массовой культуры, основанных на культе насилия, а также духовных и нравственных ценностей, противоречащих принятым в российском обществе. Эта угроза проявляется в виде деятельности граждан или их объединений по распространению идей религиозного экстремизма и нетерпимости, этнического превосходства или унижения. Распространение таких идей при отсутствии контрпропаганды со стороны общества и государства приводит к размыванию в индивидуальном и общественном сознании значимости традиционных ценностей, формированию представлений об отсутствии социальной поддержки этих ценностей.

Основу правового регулирования отношений в области противодействия этой угрозе составляет принцип закрепления в нормах права запрета на распространение и использование основных эле ментов культуры, основанной на идеях насилия, национальной и религиозной ненависти, оскорбляющих в связи с этим национальные культурные ценности российского народа, включая использование относящихся к ней символов, и юридической ответственности лиц и объединений граждан, нарушающих данный запрет.

Правовое обеспечение безопасности информации в форме сообщений определяется совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются сообщения, передаваемые по каналам связи, данные, накапливаемые и обрабатываемые в информационных системах, автоматизированных системах управления, а также документы как входящие, так и не входящие в информационные системы.

Основная цель правового регулирования в этой области состоит в предупреждении, выявлении и пресечении проявлений угроз без опасности этих объектов и минимизации последствий таких проявлений.

Основная угроза безопасности информации в форме сообщений заключается в их несанкционированной модификации, уничтожении или задержке. Эта угроза проявляется в форме соответствующих действий физических или юридических лиц.

В основу правового регулирования отношений в области противодействия данной угрозе положены следующие принципы:

- выделение социально опасных действий, направленных на нарушение безопасности сообщений (документов), передаваемых по каналам связи, данных, накапливаемых и обрабатываемых в информационных системах, в автоматизированных системах управления, и запрет этих действий под угрозой применения уголовной или административной ответственности;

- формирование механизмов установления, поддержания и снятия режимов общедоступной информации и информации органического доступа, в том числе режима тайны (коммерческой, государственной и иных охраняемых законом тайн);

- закрепление требований к информационным системам, техническим средствам передачи, обработка и хранение информации, контроль выполнения этих требований, а также установление в определенных случаях гражданской, административной и уголовной ответственности за нарушение этих требований;

- правовая охрана установленных режимов доступа к информации.

Правовое обеспечение безопасности информационной инфраструктуры образуется совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются средства связи, автоматизации обработки информации, информационно телекоммуникационные системы и средства массовой информации.

Основные угрозы безопасности информационной инфраструктуры представляют собой нарушения работоспособности и функционирования основных составляющих информационной инфраструктуры — информационных и телекоммуникационных систем, сетей связи, системы массовой информации и т.п.

Основной целью правового обеспечения безопасности информационной инфраструктуры является предупреждение, пресечение и минимизация последствий проявления этих угроз.

В основу правового регулирования отношений, связанных с обеспечением безопасности сети связи, средств автоматизации обработки информации и информационно-телекоммуникационных систем как средства взаимодействия между отдельными субъектами, положены принципы:

- установление правового режима радиочастотного спектра и государственный контроль его поддержания;

- закрепление требований к организации защиты объектов и сооружений связи и установление административной ответственности за их выполнение;

- лицензирование деятельности по предоставлению услуг связи и государственный контроль за соблюдением лицензионных условий;

- подтверждение соответствия средств связи и услуг установленным требованиям;

- запрет на распространение вредоносных программ и применение уголовной ответственности за его нарушения.

В основу правового регулирования отношений в области обеспечения безопасности функционирования средств массовой информации и информационно-телекоммуникационных систем как средства распространения массовой информации положены принципы:

- ограничение участия иностранных юридических лиц, лиц с двойным гражданством и лиц без гражданства в учреждении российских средств массовой информации;

- запрет на распространение продукции зарубежных средств массовой информации вместо продукции отечественных средств массовой информации в качестве одного из условий получения лицензии на вещание, распространение продукции средств массовой информации, возможность аннулирования лицензии на вещание в случае неоднократного нарушения лицензионных условий;

- запрет на осуществление гражданами, должностными лица ми, предприятиями, учреждениями, организациями, государственными органами действий, направленных на воспрепятствование распространению продукции СМИ, и привлечение виновных лиц к установленной законом административной ответственности.

Правовое обеспечение безопасности правового статуса субъектов информационной сферы образуется совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются:

- права человека и гражданина на участие в информационных отношениях (на свободу поиска, получения, передачи, производства и распространения информации, на свободу мысли и слова, массовой информации; на неприкосновенность частной жизни, личную и семейную тайну, на защиту своей чести и доброго имени, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и др.);

- обязанности граждан, возникающие в связи с участием в информационных отношениях (непротиводействие реализации конституционных прав и свобод в области информации; соблюдение запретов пропаганды и агитации, возбуждающих расовую, национальную, религиозную ненависть и вражду; забота о сохранении культурного наследия).

Основными угрозами безопасности правового статуса субъектов информационной сферы являются нерациональное ограничение доступа к общественно необходимой информации, открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, другой открытой социально значимой информации, манипулирование информацией, противодействие реализации гражданами их права на личную и семейную тайны, тайну переписки, телефонных переговоров и иных сообщений, а также нарушение других законных ограничений на сбор и распространение информации.

Основной целью правового обеспечения безопасности правового статуса субъектов информационной сферы является предупреждение, пресечение и минимизация последствий проявления этих угроз.

В основу правового регулирования отношений, связанных с обеспечением безопасности правового статуса субъектов информационной сферы, положены следующие принципы:

- закрепление государственных гарантий доступа к общедоступной информации, в том числе к информации о деятельности государственных органов, органов местного самоуправления;

- установление требований к созданию и функционированию государственных информационных систем и информационных систем органов местного самоуправления;

- законодательное закрепление порядка и условий автоматизированной обработки персональных данных;

- закрепление порядка использования электронной цифровой подписи в электронном документообороте для обмена юридически значимыми электронными документами.

Содержание и структура законодательства

Правовые нормы и институты, образующие правовое обеспечение информационной безопасности, закрепляются в нормативных правовых актах, являющихся источниками права в этой области и составляющих соответствующее законодательство.

В Конституции Российской Федерации закреплены следующие права и свободы: право каждого свободно искать, получать, передавать, производить и распространять информацию любым за конным способом; право на неприкосновенность частной жизни, личную и семейную тайну; право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы; запрет на сбор, хранение и распространение информации о частной жизни лица без его согласия и другие нормы.

Федеральные законы закрепляют значительное количество норм, регулирующих отношения в области обеспечения информационной безопасности. К числу данных законов относятся Федеральный конституционный закон «О Правительстве Российской Федерации», Федеральный конституционный закон «Об Уполномоченном по правам человека в Российской Федерации», Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Налоговый кодекс Российской Федерации, Трудовой кодекс Российской Федерации, Таможенный кодекс Российской Федерации и др.

Так, Гражданский кодекс Российской Федерации закрепляет нормы, регулирующие отношения в области защиты конфиденциальной информации и некоторых иных видов тайн (коммерческой тайны, личной и семейной тайны), признания электронной цифровой подписи средством удостоверения сделки.

Кодекс Российской Федерации об административных правонарушениях устанавливает ответственность за отказ в предоставлении гражданину информации, за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных), за нарушение правил защиты информации, за незаконную деятельность в области защиты информации и другие некоторые правонарушения.

Уголовный кодекс Российской Федерации устанавливает ответственность за нарушение неприкосновенности частной жизни, тайны переписки и телефонных переговоров, отказ в предоставлении гражданину информации, незаконный экспорт научно- технической информации, разглашение государственной тайны, преступления в сфере компьютерной информации и другие преступления в данной сфере.

Важную роль в правовом регулировании отношений в области обеспечения информационной безопасности играют такие основополагающие нормативные правовые акты, как законы Российской Федерации «О безопасности», «О средствах массовой ин формации», «О государственной тайне», Патентный закон Российской Федерации, федеральные законы «Об информации, информационных технологиях и о защите информации», «Об электронной подписи» и др.

Среди нормативных правовых актов Президента Российской Федерации можно выделить указы Президента Российской Федерации «О снятии ограничительных грифов с законодательных и иных актов, служивших основанием для массовых репрессий и посягательств на права человека», «О дополнительных правах граждан на информацию», «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти» и др. Кроме того, важной составляющей рассматриваемого законодательства являются указы Президента Российской Федерации, устанавливающие компетенцию федеральных органов исполнительной власти в рассматриваемой области.

Подзаконные акты Правительства Российской Федерации, других федеральных органов исполнительной власти, принятые по отнесенным к их компетенции вопросам и относящиеся к пред мету правового обеспечения информационной безопасности, в частности, включают постановления Правительства Российской Федерации «Об упорядочении использования радиоэлектронных средств (высокочастотных устройств) на территории Российской Федерации», «О порядке изготовления, приобретения, ввоза в Российскую Федерацию и использования на территории Российской Федерации радиоэлектронных средств (высокочастотных устройств)», «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» и др.

Существует значительное количество правовых актов, принятых Гостехкомиссией России (в настоящее время функции уполномоченного федерального органа исполнительной власти в этой области исполняет ФСТЭК России) по вопросам защиты информации. Так, вопросы защиты информации затрагиваются в руководящих документах Гостехкомиссии России («Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» 1992 г., «Защита от НСД. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровням контроля отсутствия недекларированных возможностей» 1998 г. и др.).

Кроме того, к источникам права в этой области могут относиться решения Конституционного Суда Российской Федерации, разъяснения Верховного Суда Российской Федерации и Высшего Арбитражного Суда Российской Федерации.

Важной составляющей законодательства в области обеспечения информационной безопасности являются также международные договоры Российской Федерации.

Структура законодательства в области правового обеспечения информационной безопасности и структура нормативного правового обеспечения информационной безопасности в определенной степени различаются. Это обусловлено тем, что система права и система законодательства, образуя совместно объективное право, имеют разные назначение и механизмы развития. В системе права отражается содержание права как регулятивной системы,

состоящей из норм права, правовых институтов и отраслей права. Она выступает объективным основанием системы законодательства.

В свою очередь, система законодательства призвана закрепить правовые нормы в системе нормативных правовых актов, взаимосвязанных по предмету правового регулирования и их юридической силе.

В отличие от системы права, складывающейся в соответствии с исторически обусловленной структурой общественных отношений, система законодательства является продуктом рациональной деятельности людей, осуществляемой во времени и пространстве.

Система законодательства, как и система права, подразделяется на отрасли — наиболее крупные объединения нормативных актов и их частей по определенным сферам правового регулирования.

Элементами системы законодательства являются нормативные правовые акты, а также их структурные составляющие (разделы, главы, статьи пункты и т.д.), которые могут объединяться в раз личные композиции, выделенные по определенному основанию из всей совокупности признаков и характеристик объекта.

Структуру законодательства в области обеспечения информационной безопасности удобно представлять в качестве системы законодательных отраслей права, включающих, в частности:

- законодательство об информации, информационных техно логиях и о защите информации;

- законодательство о персональных данных;

- законодательство об интеллектуальной собственности;

- законодательство о тайнах;

- законодательство о средствах массовой информации и о рекламе;

- законодательство о связи;

- законодательство о техническом регулировании;

- законодательство об электронной подписи.

Задание:

Используя теоретический материал, подготовить отчет включающий ответы на контрольные вопросы.

Контрольные вопросы:

1. Что такое «правовое обеспечение информационной безопасности» и в чем заключается его предмет?
2. Раскройте понятие «субъекта и объекта правоотношений в области защиты информации».

3. Опишите содержание правового обеспечения безопасности сведений, сообщений и информационной инфраструктуры.
4. Раскройте содержание и структуру законодательства в области обеспечения информационной безопасности (включая описание иерархии правовых актов).

Лабораторная работа №2

Тема: Компьютерная система как объект информационной безопасности

Цель работы:

- исследование терминологической базы

- закрепление знаний основного понятийного аппарата, применяемого в области защиты информации

- формирование навыка работы с нормативными документами по исследуемому вопросу

- описание выбранного объекта защиты информации для дальнейшего исследования

Теоретическая часть:

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем является одним из ведущих направлений развития информационных технологий. В ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» приведены основные понятия защиты информации и информационной безопасности компьютерных систем.

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты — информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Цель защиты информации — заранее намеченный результат защиты информации.

Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации — степень соответствия результатов защиты информации поставленной цели.

Защита информации от утечки — защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглаше-

ния и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Защита информации от разглашения — защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от НСД — защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Система защиты информации — совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации. Под информационной безопасностью понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной. Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, и стихийные бедствия (землетрясение, ураган, пожар) и т. п.

Современная автоматизированная система (АС) обработки информации представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты АС можно разбить на следующие группы:

• аппаратные средства — компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства — дисководы, принтеры, контроллеры, кабели, линии связи и т. д.);

• программное обеспечение — приобретенные программы, исходные, объектные, загрузочные модули; ОС и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;

• данные — хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;

• персонал — обслуживающий персонал и пользователи.

Одной из особенностей обеспечения информационной безопасности в АС является то, что таким абстрактным понятиям, как информация, объекты и субъекты системы, соответствуют физические представления в компьютерной среде:

• для представления информации — машинные носители информации в виде внешних устройств компьютерных систем (терминалов, печатающих устройств, различных накопителей, линий и каналов связи), оперативной памяти, файлов, записей и т. д.;

• объектам системы — пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к содержащейся в нем информации;

+• субъектам системы — активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы. Информационная безопасность компьютерных систем достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы. Перечисленные выше базовые свойства информации нуждаются в более полном толковании.

Рекомендуемые источники:

1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
2. Стратегия развития информационного общества в Российской Федерации, утверждённая Президентом Российской Федерации 07.02.2008 № Пр-212.
3. Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 - ФЗ "О безопасности"
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»
5. «Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утверждено постановлением Совета Министров – Правительства Российской Федерации от 15.09.1993 г. № 912-51.
6. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
7. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
8. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
9. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
10. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
11. Федеральный закон РФ от 29 июля 2004 г № 98-ФЗ «О коммерческой тайне».
12. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
13. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
14. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
15. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.

16. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
17. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации Решение председателя Гостехкомиссии России от 25 июля 1997 г.
18. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом Гостехкомиссии России от 19 июня 2002 г. № 187 (часть 1, часть 2, часть 3).
19. Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности, Гостехкомиссия России, 2003 год.
20. Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты, Гостехкомиссия России, 2003 год.
21. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты, Гостехкомиссия России, 2003 год.
22. Руководство по разработке профилей защиты и заданий по безопасности, Гостехкомиссия России, 2003 год.
23. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России.
24. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России.
25. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России.
26. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России.
27. ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России.
28. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.
29. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.
30. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России.
31. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России.
32. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России.

Задание (оформить в виде отчета):

1. Выбрать объект защиты информации (ОЗИ) из предложенного перечня.
2. Указать наименование и назначение ОЗИ.
3. Описать пространственную модель ОЗИ, включающую (в качестве основы можно взять таблицу из приложения №1):

- описание помещения, где находится ОЗИ,
- инженерные конструкции,

- коммуникации,
- средства связи,
- основные параметры электронных устройств, находящихся в одном помещении с ОЗИ,
- технические средства безопасности.

Наименование объекта защиты информации:

1. Одиночно стоящий компьютер в бухгалтерии.
2. Сервер в бухгалтерии.
3. Почтовый сервер.
4. Веб-сервер.
5. Компьютерная сеть материальной группы.
6. Одноранговая локальная сеть без выхода в Интернет.
7. Одноранговая локальная сеть с выходом в Интернет.
8. Сеть с выделенным сервером без выхода в Интернет.
9. Сеть с выделенным сервером с выхода в Интернет.
10. Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.
11. Телефонная сеть.
12. Средства телекоммуникации (радиотелефоны, мобильные телефоны, пейджеры).
13. Банковские операции (внесение денег на счет и снятие).
14. Операции с банковскими пластиковыми карточками.
15. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
16. Компьютер, хранящий конфиденциальную информацию о разработках предприятия.
17. Материалы для служебного пользования на твердых носителях в производстве.
18. Материалы для служебного пользования на твердых носителях на закрытом предприятии.
19. Материалы для служебного пользования на твердых носителях в архиве.
20. Материалы для служебного пользования на твердых носителях в налоговой инспекции.

Приложение №1

Пример оформления пространственной модели контролируемых зон

№ п.п	Пространственная характеристика помещения	Функциональная, конструктивная и техническая характеристика помещения		
1	Этаж	2	Площадь, $м^2$	56
2	Количество окон, тип сигнализации, наличие штор на окнах	3 окна, жалюзи на окнах, плотные шторы, датчики разбития стекла «Breakglass 2000», F2, Y2, M1:2	Куда выходят окна	Проспект Мира

3	Двери, кол-во, одинарные, двойные	4 двери звукоизолирующие тяжелые	Куда выходят двери	Коридор, каб. №3, каб. №2, каб. №1
4	Соседние помещения, название, толщина стен	1.С западной стороны находится Помещение №3. отштукатуренная с двух сторон стена (толщина - 1,5 кирпича) 2. С восточной стороны расположен коридор. отштукатуренная с двух сторон стена (толщина - 1,5 кирпича)		
5	Помещение над потолком, название, толщина перекрытий	Отсутствует		
6	Помещение под полом, название, толщина перекрытий	1.Складское помещение. Бетонная плита 30 см, изоляционная ткань, паркет		
7	Вентиляционные отверстия, места размещения, размеры отверстий	Отсутствуют		
8	Батареи отопления, типы, куда выходят трубы	Централизованное, восьми секционные, трубы выходят на 1 этаж		
9	Цепи электропитания	Напряжение, (В), количество розеток электропитания, входящих и выходящих кабелей	220 В 7 розеток 2 входящих телефонных кабелей, 1 входящий АСУ	
10	Телефон	Типы, места установки телефонных аппаратов, тип кабеля	1. ТА-68, зав. № 0076, Т3	
11	Радиотрансляция	Типы громкоговорителей места установки	1. Громкоговоритель «LBC3087/31»,N24	
12	Электрические часы	Тип, куда выходит кабель электрических часов	1.Часы «Gastar SP 3340 Red», N1:17, выходит к электрическому щиту в коридоре	
13	Бытовые радиосредства	Радиоприемники, телевизоры, аудио и видеомагнитофоны, их кол-во и типы	Отсутствуют	
14	Бытовые электроприборы	Вентиляторы и др., места их размещения	Отсутствуют	
15	ПЭВМ	Кол-во, типы. состав, места размещения	1.системный блок, зав. № 0076, V1:16; 2. монитор Samsung, зав. № 0716, V1:15; 3.клавиатура, зав. № 276, V1:15.	
16	Технические средства охраны	Типы и места установки извещателей, зоны действий излучений	датчики движения:	

			1. «Контроль-Люкс 360°», 12 м, H1:10; H14; 2. «M-901A»,12 м, V12; D1:19;
17	Телевизионные средства наблюдения	Места установки, типы и зоны наблюдения телевизионных трубок	Видеокамеры: 1. «LCL-217 HS», 176 г., B26; X1:12.
18	Пожарная сигнализация	Типы извещателей, схемы соединения и вывода шлейфа	Пожарные датчики 1. «ИП 212/101-4-A1R», N1:10; 2.«ИП212/101-2», H7, Z7. 3. Извещатель пожарный ручной «ИПР 513-3А», X24
19	Другие средства		Отсутствуют

Лабораторная работа №3

Тема: Допуск должностных лиц и граждан к государственной тайне

Цель работы:

- закрепление теоретических знаний в области правового обеспечения информационной безопасности

- ознакомление с понятием «государственная тайна»

- закрепление знаний основного понятийного аппарата, применяемого в области защиты информации

- формирование навыка работы с нормативными документами по исследуемому вопросу

- формирование навыков оформления документов на получение допуска к государственной тайне

Рекомендуемая литература:

1. Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне"
2. Указ Президента РФ от 30 ноября 1995 г. № 1203 "Об утверждении перечня сведений, отнесенных к государственной тайне"

3. Постановление Правительства РФ от 06.02.2010 N 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"
4. ФЗ РФ от 28 декабря 2010 г. N 390-ФЗ "О безопасности"

Теоретическая часть:

В настоящее время информация является одним из наиболее ценных ресурсов. Научные знания и технологии, которыми располагает государство, определяют его стратегический потенциал и влияние в мире. Как правило, подобного рода информация относится к категории *государственной тайны* и охраняется государственными институтами.

Институт государственной тайны является неотъемлемой составляющей общественной жизни, частью правовой системы. Государственные средства воздействия на информационные процессы – важнейшее политическое условие обеспечения прав человека и рационализации использования информационных ресурсов в обществе. Система защиты секретов – наиболее сильное звено государственного влияния в информационной сфере. Сведения, составляющие государственную тайну, имеют особую важность для общества и государства.

Государственная секретность в той или иной степени присутствует во всех развитых странах мира. В качестве угрозы своей безопасности государство, как правило, рассматривает потенциальную утечку защищаемой информации за границу. При этом величина возможного ущерба от разглашения государственной тайны занимает приоритетное место в системе национальной безопасности государства. Сохранению наиболее важных секретов государства уделяется приоритетное значение, для чего устанавливается особый режим защиты государственной тайны.

Правовой институт государственной тайны имеет три составляющие:

1) сведения, относимые к определенному типу тайны;

2) режим секретности как механизм ограничения доступа к указанным сведениям;

3) санкции за неправомерное получение и (или) распространение этих сведений.

Понятие «государственная тайна» является одним из важнейших в системе защиты государственных секретов. От правильного толкования данного понятия во многом зависит политика руководства страны в области информационной безопасности. Как правило,

в данном определении указываются категории сведений, которые защищаются государством, и сообщается, что распространение этих сведений может нанести ущерб интересам государственной безопасности.

Законодательство Российской Федерации о государственной тайне основывается на *Конституции Российской Федерации*, законе Российской Федерации *«О безопасности»* и включает закон *«О государственной тайне»,* а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Кроме того, данным законом определяется *Перечень сведений составляющих государственную тайну*, который конкретизируется Указом Президента РФ в *«Перечне сведений, отнесенных к государственной тайне»*. К ним отнесены сведения (указаны лишь разделы): в военной области; о внешнеполитической и внешнеэкономической деятельности; в области экономики, науки и техники; в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Критерии для отнесения сведений к государственной тайне определены *Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности.*

К *сведениям особой важности* следует относить такие сведения, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких областях.

К *совершенно секретным сведениям* следует относить такие сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики Российской Федерации в одной или нескольких областях.

К *секретным сведениям* следует относить все иные из числа сведений, составляющих государственную тайну. Ущерб может быть нанесен интересам предприятия, учреждения или организации.

В зависимости от вида, содержания и размеров ущерба выделяются группы некоторых видов ущерба при утечке сведений, составляющих государственную тайну.

Политический ущерб может наступить при утечке сведений политического и внешнеполитического характера, о разведывательной деятельности спецслужб государства и др. Политический ущерб может выражаться в том, что в результате утечки информации могут произойти серьезные изменения в международной обстановке не в пользу Российской Федерации, утрата страной политических приоритетов в каких-то областях, ухудшение отношений с какой-либо страной или группой стран и т.д.

Экономический ущерб может наступить при утечке сведений любого содержания: политического, экономического, военного, научно-технического и т.д. Экономический ущерб может быть выражен, прежде всего, в денежном исчислении. Экономические потери от утечки информации могут быть прямые и косвенные.

Так, прямые потери могут наступить в результате утечки секретной информации о системах вооружения, обороны страны, которые в результате этого практически потеряли или утратили свою эффективность и требуют крупных затрат на их замену или переналадку. Косвенные потери чаще всего выражаются в виде размера упущенной выгоды: срыв переговоров с иностранными фирмами, о выгодных сделках с которыми ранее была договоренность; утрата приоритета в научном исследовании, в результате чего соперник быстрее довел свои исследования до завершения и запатентовал их, и т.д.

Моральный ущерб, как правило, неимущественного характера, наступает от утечки информации, вызвавшей или инициировавшей противоправную государству пропагандистскую кампанию, подрывающую репутацию страны, приведшую к ухудшению дипломатических связей государств, высылке дипломатов, разведчиков, действовавших под дипломатическим прикрытием, и т. п.

Современные интеграционные процессы, связанные с развитием международных экономических, политических, культурных связей приводят к открытости отношений государств, необходимости максимально возможного сокращения числа сведений, относимых к государственной тайне. В то же время обязанностью любого государства является формирование оптимального механизма защиты различных видов информации и определения принципов функционирования института государственной тайны. Такие требования исходят, с одной стороны, из потребности современного общества быть более открытым и доступным, а с другой — диктуются необходимостью обеспечения безопасности личности, общества и государства.

Система защиты государственной тайны

В 2000 г., с принятием Доктрины информационной безопасности Российской Федерации была организована *Система обеспечения информационной безопасности Российской Федерации*, которая является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются: Президент Российской Федерации, Совет Федерации Федерального собрания Российской Федерации, Государственная дума Федерального собрания Российской Федерации, Правительство Российской Федерации, Совет

Безопасности Российской Федерации, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации.

Президент Российской Федерации руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации; санкционирует действия по обеспечению информационной безопасности Российской Федерации; в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности Российской Федерации; определяет в своих ежегодных посланиях Федеральному собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации настоящей Доктрины.

Палаты Федерального Собрания Российской Федерации на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формируют законодательную базу в области обеспечения информационной безопасности Российской Федерации.

Правительство Российской Федерации в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Российской Федерации Федеральному собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности Российской Федерации проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, оперативно подготавливает проекты решений Президента Российской Федерации по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности Российской Федерации, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента Российской Федерации в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту Российской Федерации и Правительству Российской Федерации.

Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации.

Система защиты сведений, отнесенных к государственной тайне, и их носителей складывается из:

♦ органов защиты государственной тайны;

♦ средств и методов защиты государственной тайны;

♦ проводимых мероприятий.

В 2004 г., в связи с реорганизацией системы государственной службы Российской Федерации, «Гостехкомиссия» России была преобразована в *Федеральную службу по техническому и экспертному контролю (ФСТЭК)*, которая является на сегодняшний день ключевым элементом структуры государственной системы защиты информации.

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

В настоящее время *в структуру государственной системы защиты информации* входят:

♦ Федеральная служба по техническому и экспортному контролю (ФСТЭК);

♦ территориальные органы ФСТЭК;

♦ Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России (головная научная организация по проблемам защиты информации), а также другие подведомственные ФСТЭК России организации;

♦ ФСБ, МО, МВД, СВР, ФАПСИ при Президенте РФ, и их подразделения по защите информации;

♦ структурные и межотраслевые подразделения по защите информации органов государственной власти;

♦ головные и ведущие НИИ, проектные и конструкторские организации органов государственной власти;

♦ предприятия, проводящие работы с использованием сведений, составляющих государственную и служебную тайну, и их подразделения по защите информации;

♦ предприятия, специализирующиеся на проведении работ в области защиты информации;

Задание:

1. Используя теоретический материал, подготовить отчет включающий ответы на контрольные вопросы.
2. Опишите поэтапно порядок допуска должностных лиц и граждан РФ к государственной тайне.
3. Используя Инструкцию о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне, оформить все необходимые документы для поучения соответствующего допуска.

Лабораторная работа № 4.

Тема: Организация службы защиты информации на предприятии

2.1. Цель работы

Изучение организационных основ защиты информации (ЗИ) на предприятии.

2.2. Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

- изучить теоретический материал по выявлению угроз и методам их устранения на предприятии;
- разделиться на подгруппы и распределить должности;
- дать характеристику выбранного предприятия и выделить основные виды защищаемой информации на предприятии;
- спроектировать и начертить структуру службы защиты информации, разработать модель угроз и модель нарушителя информационной безопасности;
- описать основные организационные задачи и функциональные обязанности по каждой из представленных должностей: зам. руководителя предприятия по безопасности, юрисконсульт по безопасности, аналитик, сотрудник службы управления персоналом, сотрудник подразделения экономической контрразведки, сотрудники сектора технической защиты, администратор безопасности системы и сотрудник сектора охраны и режима;
- выполнить требования для рассматриваемой должности.

2.3. Краткие теоретические сведения

Успех в производственной и предпринимательской деятельности в немалой степени зависит от умения распоряжаться таким товаром, как информация. Служба защиты информации является основным органом управления ЗИ и координатором деятельности по обеспечению безопасности информации на предприятии.

2.3.1. Состав службы безопасности предприятия

Служба безопасности является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия. Такая структура управления системой безопасности имеет чёткую вертикаль и характерна для обеспечения безопасности, где требуются определенность, явно обозначенные границы, регламентация отношений на всех уровнях.

Решение о создании системы безопасности принимается руководством предприятия в соответствии с ее уставом. Руководитель предприятия должен хорошо знать, что подлежит защите.

Перед руководителем предприятия остро встают два вопроса:

- сохранение материальных ценностей;
- обеспечение защиты информации, в том числе сведений, составляющих коммерческую или государственную тайну.

Все взаимоотношения работника и работодателя, начиная с момента создания службы, ее деятельности и заканчивая ее ликвидацией, строго регламентированы законодательством Российской Федерации. Твердые знания положений этих законов позволяют любому руководителю грамотно организовать деятельность вверенного в его руководство предприятия и добиться максимальной эффективности решения поставленных задач.

Функции юрисконсульта по безопасности следующая: разрабатывать, вести и обновлять основополагающие документы с целью закрепления в них требований по обеспечению безопасности и защиты конфиденциальной информации.

Возглавляет службу безопасности начальник в должности заместителя руководителя предприятия по безопасности. При этом руководитель службы безопасности должен обладать максимально возможным кругом полномочий, позволяющим ему влиять на другие подразделения и различные области деятельности предприятия, если этого требуют интересы безопасности. Деятельность службы защиты информации зависит от того, как будет организован процесс управления деятельностью службы её начальником.

Руководитель службы защиты информации должен выполнять следующие функции:

- вырабатывать политику обеспечения защиты информации и обеспечивать ее реализацию;
- отвечать за функционирование службы защиты информации и обеспечение защиты конфиденциальной информации;
- осуществлять планирование и непосредственное руководство работой службы защиты информации, нести персональную ответственность за выполнение службой возложенных на нее задач, неукоснительное исполнение подчиненными своих должностных обязанностей и правил внутреннего трудового распорядка;
- принимать личное участие в проведении наиболее сложных мероприятий по обеспечению защиты информации в компании;

- разрабатывать планы действий в чрезвычайных ситуациях, проводить регулярную учебу с подчиненными;
- руководить проведением служебных расследований;
- организовывать взаимодействие службы защиты информации с другими подразделениями;
- разрабатывать инструкции персоналу предприятия по работе со сведениями, составляющими коммерческую тайну;
- организовывать разработку рекомендаций по совершенствованию функционирования службы защиты информации;
- осуществлять руководство отделом охраны.

Структура, численность и состав службы безопасности предприятия определяются реальными финансовыми возможностями, масштабом коммерческой деятельности и степенью конфиденциальности информации. В зависимости от этих факторов служба безопасности может варьировать от двух-трех человек, работающих по совместительству, до полномасштабной службы с развитой структурой (несколько десятков и сотен человек).

Наиболее полный состав в виде отделов, групп или отдельных специалистов службы безопасности предприятия может включать следующий набор организационных структур:

- подразделение охраны;
- подразделение режима;
- подразделение по работе с кадрами;
- специальный отдел (подразделение по работе с документами, содержащими коммерческую тайну);
- подразделение инженерно-технической защиты;
- подразделение разведки;
- подразделение контрразведки;
- подразделение информационно-аналитической деятельности;
- подразделение (служба) защиты информации.

Таким образом, из структуры службы безопасности видно, что одна часть её подразделений обеспечивают физическую безопасность предприятия, а другая - информационную безопасность предприятия.

Основными задачами службы безопасности являются:

- 1) обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной;
- 2) организация работы по правовой, организационной и инженерно-технической защите коммерческой тайны;
- 3) организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;
- 4) предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;
- 5) выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных ситуациях.

2.3.2. Построение структурной схемы управления службой безопасности

Взаимосвязь и взаимодействие между объектами управления и управляющими органами могут быть представлены в виде структурных схем или структур. Опорными точками такой структуры являются:

- 1. Руководитель предприятия;
- 2. Совет по безопасности предприятия;
- 3. Служба безопасности предприятия в составе отделов: охраны, режима, кадров, документов с коммерческой тайной, инженерно-технических средств безопасности и контрразведывательной и информационно-аналитической деятельности и защиты информации;
- 4. Линейные подразделения предприятия, активно участвующие в обеспечении экономической безопасности (кадровое, финансовое, плановое, юридическое, маркетинга и др.).

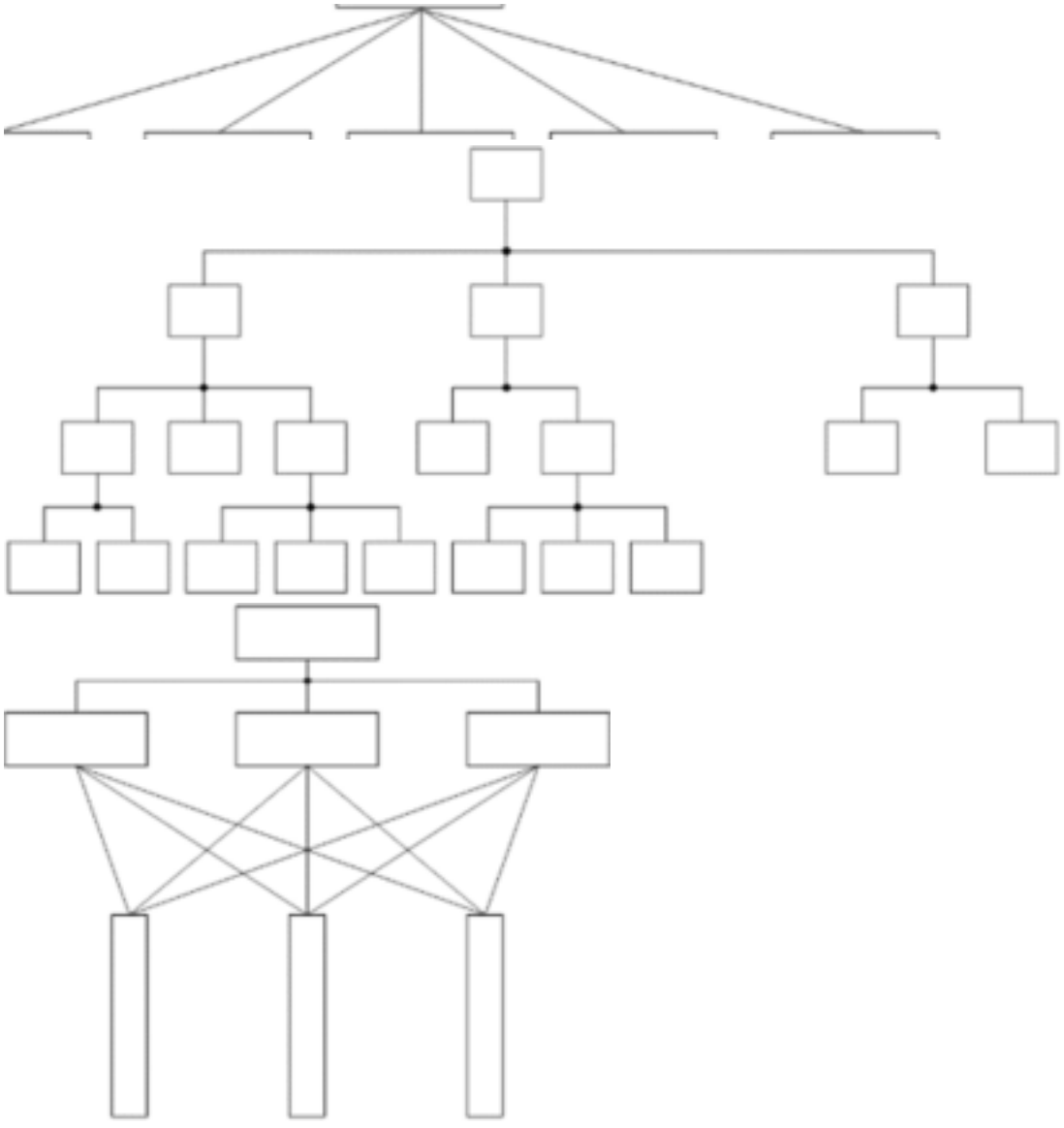

Рис 2.1. **Иерархическая однозвенная структура управления**

Рис 2.2. **Линейная иерархическая структура**

Рис. 2.3. **Функциональная структура**

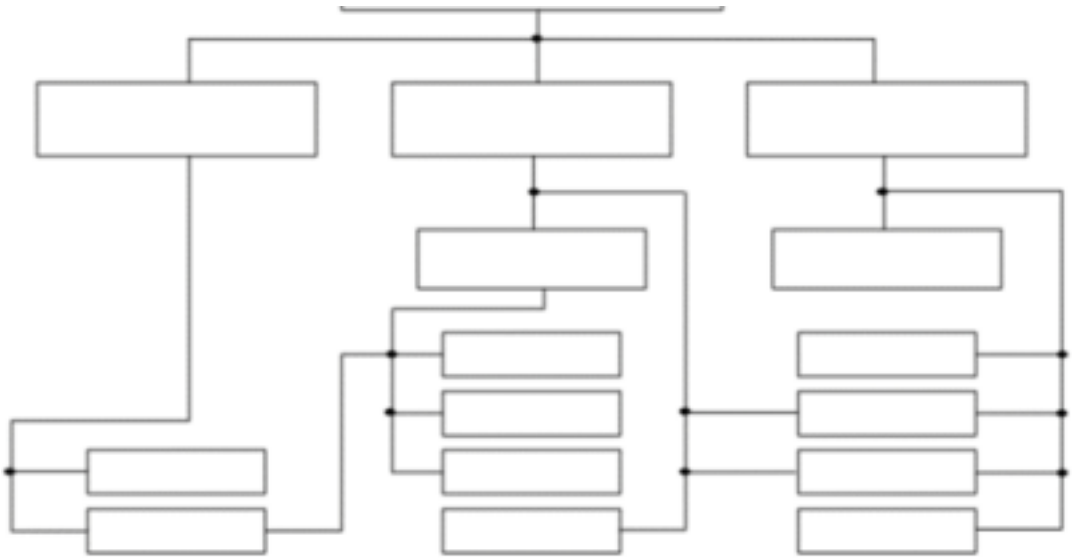

Рис. 2.4. **Линейно-функциональная структура**

В зависимости от специфики объектов управления организационные структуры могут строиться по различным схемам: иерархической однозвенной (рис. 2.1), линейной (рис. 2.2), функциональной (рис. 2.3), линейно-функциональной (рис. 2.4) или линейно-штабной.

Пример дерева целей службы безопасности предприятия представлен на рисунке 2.5.

Рис. 2.5. **Дерево целей службы безопасности предприятия (пример)**

- 2.4. **Порядок сдачи работы**
- 1. Представить отчет по выполненной работе.
- 2. Ответить на вопросы преподавателя по отчету.

- 2.5. **Требования к отчету**
- 1. В отчёте необходимо наличие титульного листа, теоретической части и практической части.
- 2. В практической части должны присутствовать характеристика предприятия (приложение 2), перечень основных видов защищаемой информации, структура службы защиты информации, модель угроз, модель нарушителя и описание основных организационных задач и функциональных обязанностей сотрудников предприятия в области защиты информации.
- 3. Индивидуальные требования:
- Заместитель руководителя предприятия по безопасности должен привести в отчете структуру службы защиты информации, дерево целей функционирования службы безопасности предприятия. Необходимо составить комплексный план, охватывающий все сферы деятельности службы безопасности. Комплексный план может включать в себя такие разделы, как организационные вопросы, обеспечение защиты информации предприятия, работа с кадрами, ресурсное обеспечение, контроль и т.д. Составить комплексный план в следующей форме:

№	Содержание планируемых мероприятий	Срок исполнения	Ответственный исполнитель	Форма представления результатов выполненного мероприятия	Отметка о выполнении

- Юрисконсульт по безопасности должен привести в отчете перечень правовых, нормативно-правовых и нормативных документов, составляющих организационную основу службы защиты информации на предприятии. Необходимо систематизировать отраслевые нормативные документы, регламентирующие вопросы защиты информации на предприятии.
- Аналитик должен привести в отчете следующие данные: прогноз вероятных устремлений конкурентов к конкретным материалам и разработкам предприятия, оценка надежности и степени защищенности предприятия от внутренних и внешних угроз. Необходимо выявить причины и обстоятельства, способствующие неправомерному овладению коммерческой информацией.
- Сотрудник службы управления персоналом должен привести в отчете результаты тестирования на оценку удовлетворённости потребностей работника методом парных сравнений. Необходимо протестировать не менее 6 работников данного предприятия.
- Сотрудник подразделения экономической контрразведки должен привести в отчете схему информационных потоков защищаемой информации. Необходимо разработать программу дезинформационных мероприятий на предприятии.

- Сотрудник сектора технической защиты должен привести в отчете границы контролируемых зон и рубежи защиты. Необходимо определить опасные с точки зрения возможности образования акустические, визуально-оптические и электромагнитные каналы утечки информации.
- Сотрудник сектора охраны и режима должен привести в отчете правила доступа на предприятие, которыми руководствуются сотрудники охраны. Необходимо выявить структурные подразделения предприятия, требующие усиленной охраны, а также описать инженерно-технические решения, применяемые для обеспечения эффективной охраны предприятия.
- Администратор безопасности системы должен привести в отчете таблицу разграничения доступа (матрицу доступа) к защищаемым ресурсам информационной системы на предприятии. Необходимо указать принципы работы и форматы файлов регистрации (журналирования) ОС, СУБД и приложений в информационной системе. Также необходимо рассмотреть вопрос организации защищенного электронного документооборота с использованием электронной подписи на предприятии.

Контрольная работа

Тема: Разработка должностных инструкций для лиц, ответственных за обеспечение информационной безопасности

Теоретическая часть:

В современных условиях перед предприятиями особо остро встает задача сохранения как материальных ценностей, так и информации, в том числе и сведений, составляющих коммерческую или государственную тайну. Беззастенчивая кража предприятиями и организациями интеллектуальной собственности друг друга стала почти массовым процессом. К этому следует добавить целенаправленные действия по сманиванию или подкупу рабочих и служащих предприятий конкурента с целью завладения секретами их коммерческой и производственной деятельности.

Для защиты коммерческих секретов предприятия создают собственные службы безопасности, важной предпосылкой создания которых является разработка их структуры, состава, положений о подразделениях и должностных инструкций для руководящего состава и сотрудников.

Служба безопасности (СБ) является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия. Такая структура управления системой безопасности, имеющая четкую вертикаль, характерна для области обеспечения безопасности, где требуется определенность, четкие границы, регламентация отношений на всех уровнях – от рядового сотрудника до менеджеров высшего звена. Как показывает практика, только на предприятиях, где проблемы безопасности находятся под постоянным контролем руководителя предприятия, достигаются наиболее высокие результаты.

Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности. При этом руководитель СБ должен обладать макси-

мально возможным кругом полномочий, позволяющим ему влиять на другие подразделения и различные области деятельности предприятия, если этого требуют интересы безопасности.

Основными задачами службы безопасности предприятия являются:

- обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной;
- организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;
- организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;
- предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;
- выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;
- обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне;
- обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;
- обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
- оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

Служба безопасности предприятия выполняет следующие общие функции:

- организует и обеспечивает пропускной и внутриобъектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;
- руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;
- участвует в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты коммерческой тайны, в частности, Устава, Коллективного договора, Правил внутреннего трудового распорядка, Положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
- разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ организует и контролирует выполнение требований «ИНСТРУКЦИИ по защите коммерческой тайны»;
- изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций, о деятельности предприятия и его клиентов, партнеров, смежников;
- организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия; разрабатывает, ведет, обновляет и пополняет «Перечень сведений, составляющих коммерческую тайну» и другие

нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;

- обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны;
- осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах условиях по защите коммерческой тайны;
- организует и регулярно проводит учебу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был осознанный подход;
- ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;
- ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;
- поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе.

Структура службы информационной безопасности

В структуру службы безопасности могут входить:

- директор (заместитель директора) или руководитель, непосредственно подчиненный главе фирмы;
- заместитель начальника службы безопасности — на некоторых предприятиях он руководит физической, а иногда и технической службами охраны;
- аналитик;
- юрист;
- специалисты в области обеспечения безопасности, экономической разведки, промышленной контрразведки;
- технические специалисты, умеющие применять специальную технику для защиты помещений;
- сотрудники физической охраны и пропускного режима (по найму), но подчиненные руководителю службы безопасности).

Условно сотрудников службы информационной безопасности можно разделить по функциональным обязанностям:

Сотрудник группы безопасности. В его обязанности входит обеспечение контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема ИС имеет своего сотрудника группы безопасности.

Администратор безопасности системы. В его обязанности входит ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (при необходимости) и за хранением резервных копий.

Администратор безопасности данных. В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.

Руководитель группы. В его обязанности входит разработка и поддержка эффективных мер защиты при обработке информации для обеспечения сохранности данных, оборудования и программного обеспечения; контроль за выполнением плана восстановления и общее руководство административными группами в подсистемах ИС (при децентрализованном управлении).

В небольших организациях функции руководителя службы обычно выполняет либо глава фирмы, либо его заместитель.

Количественный состав службы безопасности различен и зависит, прежде всего, от возможностей самой фирмы. Возможны различные варианты состава такой группы.

Кроме того, перечень необходимых знаний и навыков, а также функциональных обязанностей лиц, входящих в группу защиты информации может существенно отличаться в зависимости от назначения структуры и задач, решаемых в конкретной ИС.

К сожалению, на современном этапе отдается предпочтение физической и технической охране, время “оперативников” и аналитиков только начинается.

Задание:

1. Изучить учебный материал по данной теме
2. Разработать должностные инструкции для лиц, ответственных за обеспечение информационной безопасности.

Пример Должностной инструкции Руководителя службы безопасности предприятия

1.Общие положения

1. Начальник службы безопасности относится к категории руководителей.

2. На должность начальника службы безопасности назначается лицо, имеющее высшее профессиональное образование и стаж работы не менее 5 лет.

3. Назначение на должность начальника безопасности и освобождение от нее производится приказом директора предприятия.

4. Начальник службы безопасности должен знать:

4.1. Законы и иные нормативно-правовые акты Российской Федерации, регламентирующие охранную деятельность.

4.2. Специфику и структуру организации.

4.3. Принципы организации охраны объектов организации.

4.4. Характеристики технических средств защиты объектов от несанкционированного доступа к ним.

4.5. Тактику защиты охраняемых объектов от преступных посягательств.

4.6. Стратегию и тактику ведения переговоров с преступниками.

4.7. Современную отечественную и зарубежную технику (системы сигнализации, связи и т.п.), поддержание ее в эксплуатационном состоянии.

4.8. Характеристику технических средств защиты информации от несанкционированного доступа.

4.9. Назначение и виды связи.

4.10. Правила вхождения в связь и правила поведения в эфире.

4.11. Общие принципы оказания первой медицинской помощи; правила и нормы охраны труда, техники безопасности и противопожарной защиты.

4.12. Правила приема, сопровождения и сдачи товарно-материальных ценностей.

4.13. Правила сопровождения отдельных сотрудников организации.

5. Начальник службы безопасности в своей деятельности руководствуется:

5.1. Положением о службе безопасности.

5.2. Настоящей должностной инструкцией.

6. Начальник службы безопасности подчиняется непосредственно директору предприятия.

7. Начальник службы безопасности осуществляет руководство службой.

8. На время отсутствия начальника службы безопасности (болезнь, отпуск, командировка, пр.) его обязанности исполняет заместитель (при отсутствии такового - лицо, назначенное приказом директора предприятия), который приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

2. Должностные обязанности

Начальник службы безопасности:

1. Обеспечивает надежную защиту объектов организации от краж, хищений и других преступных посягательств, пожаров, аварий, актов вандализма, стихийных бедствий, общественных беспорядков и т.п.

2. Разрабатывает и осуществляет руководство мероприятиями по безопасности объектов.

3. Вырабатывает адекватные угрозе средства защиты и виды режимов охраны.

4. Пресекает попытки несанкционированного проникновения на охраняемый объект.

5. Отражает угрозу и способствует ликвидации вредных последствий непосредственного нападения на охраняемый объект.

6. Осуществляет проверку и оценку лояльности служащих охраняемого объекта.

7. Обеспечивает неприкосновенность перевозимых материальных ценностей, отражая попытки несанкционированного доступа к ним.

8. Осуществляет на охраняемом объекте связь с базовым органом службы охраны объекта, а в пути следования - с транспортными и территориальными органами внутренних дел.

9. В совершенстве владеет приемами рукопашного боя и самозащиты.

10. Владеет средствами индивидуальной защиты, холодным и огнестрельным оружием.

11. Пользуется различными видами связи на охраняемом объекте.

12. Обнаруживает и устраняет несложные технические неисправности в системах сигнализации и связи охраняемого объекта.

13. Обеспечивает соблюдение строгого контрольно-пропускного режима при осуществлении профилактических, ремонтных и других работ.

14. Осуществляет всемерную помощь правоохранительным и другим государственным органам в расследовании случаев преступных посягательств на охраняемые объекты.

15. Оказывает неотложную медицинскую помощь при ранениях, травмах и т.д.

3. Права

Начальник службы безопасности имеет право:

1. Знакомиться с проектами решений руководства предприятия, касающимися деятельности службы безопасности.

2. Вносить на рассмотрение руководства предприятия предложения по улучшению деятельности службы безопасности.

3. Осуществлять взаимодействие с руководителями всех (отдельных) структурных подразделений предприятия.

4. Запрашивать от руководителей подразделений предприятия и специалистов информацию и документы, необходимые для выполнения своих должностных обязанностей.

5. Подписывать и визировать документы в пределах своей компетенции.

6. Вносить на рассмотрение руководства предприятия представления о назначении, перемещении и увольнении сотрудников службы безопасности; предложения об их поощрении или о наложении на них взысканий.

7. Требовать от руководства предприятия оказания содействия в исполнении своих должностных обязанностей и прав.

4. Ответственность

Начальник службы безопасности несет ответственность:

1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией - в пределах, определенных действующим трудовым законодательством Российской Федерации.

2. За правонарушения, совершенные в процессе осуществления своей деятельности - в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

3. За причинение материального ущерба - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации

.

10 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

10.1 Учебно-лабораторное оборудование

Таблица 8 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
201/5	Учебная лаборатория защищённых автоматизированных систем	СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2 как для операционных систем семейства Windows так и для Linux, Ревизор Сети 2.0, Анализатор сетевого траффика Астра,Агент инвентаризации сети,Сканер сетевой безопасности XSpider, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, VipNet firewall, Etoken PKI Client, Etoken, Ноутбук с Windows 7+проектор. 16 ПЭВМ на базе процессоров не ниже Intel Pentium IV

10.2 Технические и электронные средства обучения

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Лабораторные занятия

Для лабораторных занятий используется аудитория № 201 , оснащенная оборудованием, указанным в табл. 8:

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- читальный зал НТБ КнАГУ;
- компьютерные классы (ауд. 311 корпус № 5, ауд. 205 корпус № 5, ауд. 313 корпус № 5).

11 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине
Руководство и управление службой безопасности

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Анализ безопасности информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2021*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
5	*10*	*3*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	**УК-3.1** Знает основные приемы и нормы социального взаимодействия; основные понятия и методы конфликтологии, технологии межличностной и деловой коммуникации, принципы командной работы как основы организации и руководства работой команды, способы мотивации членов команды с учетом организационных возможностей и личностных особенностей членов команды	**УК-3.2** Умеет устанавливать и поддерживать контакты, обеспечивающие успешную работу в команде; разрабатывать цели команды в соответствии с целями проекта; выбирать стратегию формирования команды и определять функциональные и ролевые критерии отбора участников	**УК-3.3** Имеет навыки организации и руководства работой команды, презентации результатов собственной и командной работы
ПК-6 Способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов	**ПК-6.1** Знает способы проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов	**ПК-6.2** Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов	**ПК-6.3** Владеет навыками проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Код контролируемой компетенции**	**Наименование оценочного средства**	**Показатели оценки**
Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности.	УК-3	Лабораторная работа 1	Умеет устанавливать и поддерживать контакты, обеспечивающие успешную работу в команде; разрабатывать цели команды в соответствии с целями проекта; выбирать стратегию формирования команды и определять функциональные и ролевые критерии отбора участников
Тема: Компьютерная система как объект информационной безопасности	ПК-6	Лабораторная работа 2	Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов
Допуск должностных лиц и граждан к государственной тайне	ПК-6	Лабораторная работа 3	Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов
Организация службы защиты информации на предприятия	ПК-6 УК-3	Лабораторная работа 4	Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов Умеет устанавливать и поддерживать контакты, обеспечивающие успешную работу в команде; разрабатывать цели команды в соответствии с целями проекта; выбирать стратегию формирования команды и определять функциональные и ролевые критерии отбора участников

Разработка должностных инструкций для лиц, ответственных за обеспечение информационной безопасности	ПК-6 УК-3	Контрольная работа	Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов Умеет устанавливать и поддерживать контакты, обеспечивающие успешную работу в команде; разрабатывать цели команды в соответствии с целями проекта; выбирать стратегию формирования команды и определять функциональные и ролевые критерии отбора участников

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 3 – Технологическая карта

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
9 семестр Промежуточная аттестация в форме зачета с оценкой				
1	Лабораторная работа 1	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Лабораторная работа 2	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала.

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
3	Лабораторная работа 3	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
4	Лабораторная работа 4	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
5	Контрольная работа-работа	В течение семестра	15 баллов	15 баллов - студент правильно выполнил задания. Показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы на защите.

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				10 баллов - студент выполнил задание с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов на защите. 5 баллов - студент выполнил задания с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено много неточностей. 0 баллов - при выполнении задания студент продемонстрировал недостаточный уровень владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено множество неточностей.
ИТОГО:			55 баллов	

Критерии оценки результатов обучения по дисциплине:
0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине);
65 – 74 % от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень);
75 – 84 % от максимально возможной суммы баллов – «хорошо» (средний уровень);
85 – 100 % от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень).

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

Методические указания приведены в соответствующем разделе.

Контрольные вопросы:

1. Назовите основные виды угроз безопасности предприятия.
2. Перечислите виды конфиденциальной информации, используемой на предприятии.
3. Какие подразделения входят в состав службы безопасности предприятия?
4. Какие требования предусматривает внутриобъектовый режим?
5. Раскройте наиболее полно понятие «государственная тайна»

6. Что означает «допуск к сведениям составляющим государственную тайну»?
7. Какие формы допуска существуют?
8. Что предусматривает допуск граждан к государственной тайте?
9. Перечислите органы безопасности РФ.
10. Что такое «правовое обеспечение информационной безопасности» и в чем заключается его предмет?
11. Раскройте понятие «субъекта и объекта правоотношений в области защиты информации».
12. Опишите содержание правового обеспечения безопасности сведений, сообщений и информационной инфраструктуры.
13. Раскройте содержание и структуру законодательства в области обеспечения информационной безопасности (включая описание иерархии правовых актов).

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД