МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра математики и физики

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ Е.И. Луковникова
«_____» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Б1.В.ДВ.07.02

НАПРАВЛЕНИЕ ПОДГОТОВКИ

01.03.02 Прикладная математика и информатика

ПРОФИЛЬ ПОДГОТОВКИ

Инженерия программного обеспечения

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

СОДЕРЖАНИЕ ПРОГРАММЫ **Стр.**

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Вид деятельности выпускника

Дисциплина охватывает круг вопросов, относящихся к научно-исследовательскому, проектному и производственно-технологическому видам профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Целью дисциплины является овладение основными принципами управления уровнем ин формационной безопасности защищаемых ресурсов организации.

Задачи дисциплины

- Получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.
- Получение студентами умений и навыков по построению моделей угроз и нарушителей и по оценке рисков информационной безопасности в организации.
- Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ПК-6	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	**знать** – принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; – способы формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций. **уметь** – разрабатывать политику информационной безопасности. **владеть** – профессиональной терминологией; – навыками формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций.
ОПК-4	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований	**знать** – основные стандарты ИБ. **уметь** – решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности. **владеть**

	информационной безопасности	– навыками применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.ДВ.07.02 Управление информационной безопасностью относится к элективной части.

Дисциплина Управление информационной безопасностью базируется на знаниях, полученных при изучении таких учебных дисциплин, как: Методы обеспечения безопасности компьютерных систем, Дискретная математика, Операционные системы, Теоретические основы информационной безопасности, Компьютерные сети.

Основываясь на изучении перечисленных дисциплин, Управление информационной безопасностью представляет основу для преддипломной практики и подготовки к государственной итоговой аттестации.

Такое системное междисциплинарное изучение направлено на достижение требуемого ФГОС уровня подготовки по квалификации бакалавр.

3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ

3.1. Распределение объема дисциплины по формам обучения

Форма обучения	*Курс*	*Семестр*	*Трудоемкость дисциплины в часах*						*Курсовая работа (проект), контрольная работа, реферат, РГР*	*Вид промежуточной аттестации*
			Всего часов	*Аудиторных часов*	*Лекции*	*Лабораторные работы*	*Семинары Практические занятия*	*Самостоятельная работа*		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Очная	4	8	108	48	24	24	-	60	-	зачет
Заочная	-									-
Заочная (ускоренное обучение)	-		-							-
Очно-заочная	-	-	-							-

3.2. Распределение объема дисциплины по видам учебных занятий и трудоемкости

Вид учебных занятий	*Трудо-емкость (час.)*	*в т.ч. в интерактивной, активной, инновационной формах, (час.)*	*Распределение по семестрам, часам*
			8
1	**2**	**3**	**4**
I. Контактная работа обучающихся с преподавателем (всего)	48	30	48
Лекции (Лк)	24	6	24
Лабораторные работы (ЛР)	24	24	24

Групповые (индивидуальные) консультации			
II.Самостоятельная работа обучающихся (СР)	60	-	60
Подготовка к лабораторным работам	40	-	40
Подготовка к зачету	20	-	20
III. Промежуточная аттестация зачет	+	-	+
Общая трудоемкость дисциплины ……. час.	108	-	108
зач. ед.	3	-	3

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий

- для очной формы обучения:

№ раз-дела и темы	*Наименование раздела и тема дисциплины*	*Трудоем-кость, (час.)*	*Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)*		
			учебные занятия		*самостоятельная работа обучающихся**
			лекции	*лабораторные работы*	
1	**2**	**3**	**4**	**5**	**7**
1.	**Система управления информационной безопасностью.**	**108**	**24**	**24**	**60**
1.1.	Анализ объекта защиты.	10	4	4	2
1.2.	Модель угроз и модель нарушителя.	10	2	2	6
1.3	Оценка рисков информационной безопасности	26	6	6	15
1.4	Политика информационной безопасности	28	6	6	15
1.5	Управление инцидентами информационной безопасности.	34	6	6	22
	ИТОГО	**108**	**24**	**24**	**60**

4.2. Содержание дисциплины, структурированное по разделам и темам

№ раздела и темы	*Наименование раздела и темы дисциплины*	*Содержание лекционных занятий*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**2**	**3**	**4**
1.	Система управления информационной безопасностью	Основные положения стандартов по проектированию, реализации и аудиту системы управления информационной безопасностью. Организация управления персоналом в контексте обеспечения информационной безопасности	Лекция-беседа (2 час)

1.1.	Анализ объекта защиты.	Технология анализа объекта защиты. Типы информационных систем. Методы оценки ущерба от реализации угроз информационной безопасности. Комплекс стандартов в области информационной безопасности.	Лекция-беседа (2час)
1.2.	Модель угроз и модель нарушителя.	Подходы к формированию модели нарушителя и модели угроз. Требования регуляторов к формированию модели нарушителя и модели угроз.	-
1.3	Оценка рисков информационной безопасности	Основные положения стандартов в области управления рисками информационной безопасности.	-
1.4	Политика информационной безопасности	Основные положения стандартов в области регламентации обеспечения информационной безопасности.	-
1.5	Управление инцидентами информационной безопасности.	Основные положения стандартов в области управления инцидентами информационной безопасности. Регламентация действий сотрудников при возникновении нештатных ситуаций.	Лекция-беседа (2час)

4.3. Лабораторные работы

№ п/п	***Номер раздела дисциплины***	***Наименование лабораторной работы***	***Объем (час.)***	***Вид занятия в интерактивной, активной, инновационной формах, (час.)***
1	**1.**	Формальное описание структуры информационной системы.	10	Работа в малой группе (10 час)
2	**1.**	Анализ и управление рисками информационной системы компании.	14	Работа в малой группе (14 час)
		ИТОГО	**24**	**24**

4.4. Семинары/ практические занятия

Учебным планом не предусмотрено.

4.5 Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат

Учебным планом не предусмотрено.

5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Компетенции / *№, наименование разделов дисциплины*	*Кол-во часов*	*Компетенции*		*Σ комп.*	$t_{ср}$, *час*	*Вид учебных занятий*	*Оценка результатов*
		ОПК	*ПК*				
		4	**6**				
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1. Система управления информационной безопасностью	108	+	+	2	54	Лк, ЛР, СР	зачет
всего часов	**108**	**54**	**54**	**2**	**54**		

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Сычев Ю.Н. Основы информационной безопасности: учебно-практическое пособие/Ю.Н. Сычев.-М.: Изд. центр ЕАОИ, 2010.-328 с.

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№	*Наименование издания*	*Вид занятия* (*Лк, ЛР*)	*Количество экземпляров в библиотеке*, шт.	*Обеспеченность*, (экз./ чел.)
1	2	3	4	5
Основная литература				
1.	Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=438331	*Лк, ЛР, СР*	1 (ЭУ)	1
2.	Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=362895	*Лк, ЛР, СР*	1 (ЭУ)	1
3.	Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.-СПб.: изд-во Политехн. уни-та, 2014.-322 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=363040	*Лк, ЛР, СР*	1 (ЭУ)	1
Дополнительная литература				
4.	Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605	*Лк, ЛР, СР*	1 комплект	
5.	Загинайлов Ю.Н. Теория информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=276557	*Лк, ЛР, СР*	1 (ЭУ)	1

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО - ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В процессе обучения студенты могут использовать общие ресурсы:

1.Электронный каталог библиотеки БрГУ
http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=.

2. Электронная библиотека БрГУ
http://ecat.brstu.ru/catalog .

3. Электронно-библиотечная система «Университетская библиотека online» http://biblioclub.ru

.4. Электронно-библиотечная система «Издательство «Лань»
http://e.lanbook.com .

5. Информационная система "Единое окно доступа к образовательным ресурсам"
http://window.edu.ru .

6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru .

7. Университетская информационная система РОССИЯ (УИС РОССИЯ)
https://uisrussia.msu.ru/ .

8. Национальная электронная библиотека НЭБ
http://xn--90ax2c.xn--p1ai/how-to-search /.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Обучающийся должен разработать собственный режим равномерного освоения дисциплины. Подготовка студента к предстоящей лекции включает в себя ряд важных познавательно-практических этапов:

– чтение записей, сделанных в процессе слушания и конспектирования предыдущей лекции, вынесение на поля всего, что требуется при дальнейшей работе с конспектом и учебником;

– техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств);

– выполнение практических заданий преподавателя;

– знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе.

Успешность выполнения лабораторных работ определяется подготовкой к ним. Подготовка к лабораторным работами содержит:

- изучение теоретического материала, содержащегося в учебной литературе, изучение лекционного материала,

- знакомство с заданиями на лабораторную работу;

- составление плана выполнения лабораторной работы.

Наиболее продуктивной является самостоятельная работа в библиотеке, где доступны основные и дополнительные печатные и электронные источники.

При выполнении приведенных выше рекомендаций подготовка к зачету сведется к повторению изученного и совершенствованию навыков применения теоретических положений и различных методов решения к стандартным и нестандартным заданиям.

9.1. Методические указания для обучающихся по выполнению лабораторных работ

Лабораторная работа №1 Формальное описание структуры информационной системы.

Цель работы:

Описать информационный процесс, рассмотреть угрозы, выбрать организационные и технические средства защиты.

Задание:

1. Построить модели информационных систем, определить элементы информационных

систем, подверженных угрозам.

2. Преобразовать структуры информационных систем за счет добавления средств защиты информации, нейтрализующих данные угрозы.

Варианты заданий:

анализ информационных систем «Торрент-трекер»

анализ информационных систем «Интернет-магазин»

анализ информационных систем «Социальная сеть»

анализ информационных систем «Электронная почта»

анализ информационных систем «Сайт, посвященный компьютерным играм»

Порядок выполнения:

1. Используемые средства – схематичные способы представления систем и процессов, IDEF0 . Представлен пример разбора информационного процесса, черный ящик.

Рисунок 1 – Разбор информационного процесса, черный ящик

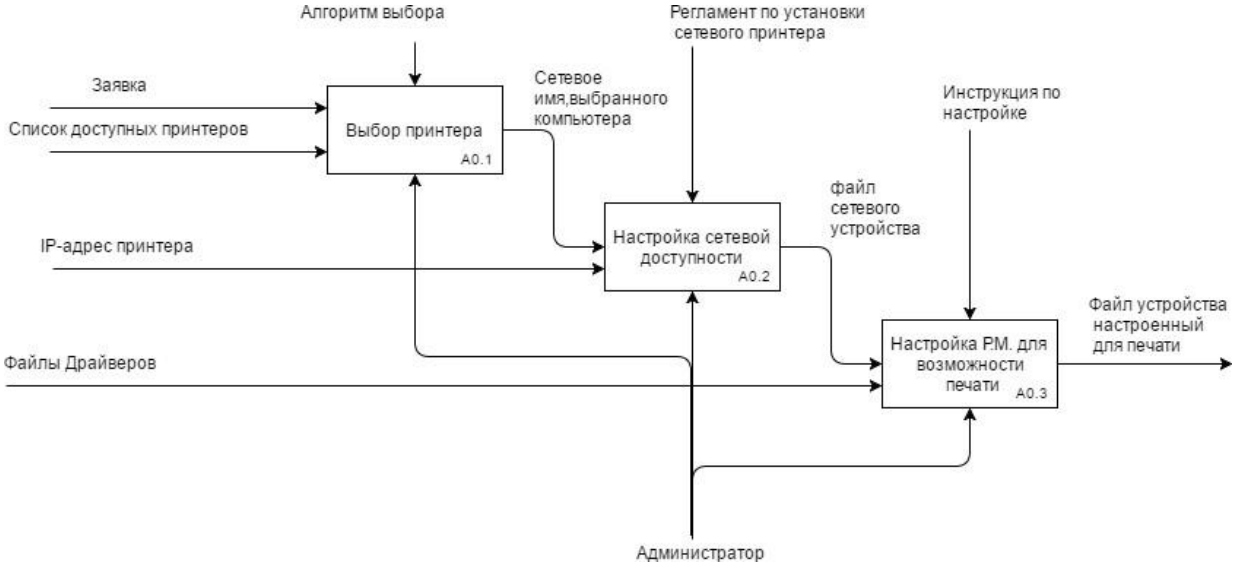

Рисунок 2 – Разбор информационного процесса, декомпозиция черного ящика

2. Пример определения элементов информационных систем, подверженных угрозам.

Таблица 1 – Угрозы и средства защиты

Под процесс	Угрозы	Средства Защиты
Заявка	Конфиденциальности: разглашение информации о заявке в электронном виде (информация о грифе печатных документов);	Орг: Подписка о неразглашении, разграничение доступа к завявке.
		Тех: Периодическая проверка контрольных сумм файлов, резервное копирование,
	Целостность: Подмена личности указанной в заявке;	Орг: Разграничение доступа;
		Тех: Периодическая проверка контрольных сумм файлов, резервное копирование;
Список доступных принтеров	Конфиденциальность:-;	Орг:-;
		Тех: -;
	Целостность: Удаление\изменение ;	Орг: разграничение доступа к списку доступных принтеров;
		Тех: Периодическая проверка контрольных сумм файлов, резервное копирование.
IP –адрес принтера	Конфиденциальность: раскрытие ip-адреса;	Орг: Подписка о неразглашении, разграничения доступа к управления настройками сети.
		Тех: Фильтрация трафика исходящего, входящего, сегментация внутренней сети, настройка Access листов, установка единственного IP адреса во внешнею сеть;
	Целостность: подмена ip-адреса;	Орг: разграничение доступа к управления настройками сети;
		Тех: Фильтрация трафика исходящего, входящего, сегментация внутренней сети, периодическая проверка MAC адресов в выбранном сегменте, настройка Access листов;
Файлы драйверов	Конфиденциальность: разглашение версии драйвера;	Орг: Подписка о неразглашении.
		Тех: -;

	Целостность: модификация драйвера	Орг: Разграничения
	злоумышленником;	доступа к управлению настройками системы.
		Тех: Периодическая проверка контрольных сумм файлов, резервное копирование.
Алгоритм выбора	Конфиденциальность: раскрытие списка секретных принтеров;	Орг: Подписка о неразглашении, инструкция правильного использования алгоритма выбора принтера;
		Тех: -;
	Целостность: удаление\изменение алгоритма выбора;	Орг: Инструкция об использовании алгоритма
		Тех: Аудит на добавление принтера;
Регламент по установке сетевого принтера	Конфиденциальность: разглашение информации о регламенте;	Орг: Подписка о неразглашении, разграничение доступа к регламенту;
		Тех: -;
	Целостность: удаление\изменение регламента;	Орг: Разграничение доступа к регламенту;
		Тех: Периодическая проверка контрольных сумм файлов, резервное копирование;
Инструкция по настройки принтера	Конфиденциальность: разглашение информации по инструкции;	Орг: Подписка о неразглашении, разграничение доступа к инструкции;
		Тех: -;
	Целостность: удаление\изменение инструкции;	Орг: Разграничение доступа к инструкции;
		Тех: Периодическая проверка контрольных сумм файлов, резервное копирование;
Сетевое имя выбранного компьютера	Конфиденциальность: разглашение информации о сетевом имени компьютера;	Орг: Подписка о неразглашении;
		Тех:-;
	Целостность: удаление\изменение сетевого имени компьютера;	Орг: Разграничение доступа к настройкам сети;
		Тех: Реализация разграничения доступа;
Файл сетевого устройства	Конфиденциальность: разглашение информации о файле сетевого устройства;	Орг: Подписка о неразглашении,
		Тех: -;

	Целостность: удаление\изменение файла сетевого устройства;	Орг: Разграничение доступа к управлению настройками сети;
		Тех: Периодическая проверка контрольных сумм файлов, резервное копирование;
Администратор	Конфиденциальность: разглашение информации об администраторе;	Орг: Подписка о неразглашении, разграничение доступа к персональным данным администратора
		Тех: -
	Целостность: урон от болезни здоровью администратора с последующим выходом из строя администратора.	Орг: Периодическое обследование сотрудников, вакцинация сотрудников;
		Тех: -;.
Файл устройства, настроенный для печати	Конфиденциальность: разглашение информации о файле устройства настроенного для печати	Орг: Подписка о неразглашении.
		Тех: -;.
	Целостность: удаление\изменение файла устройства настроенного для печати.	Орг: Разграничение доступа к настройкам системы.
		Тех: Периодическая проверка контрольных сумм файлов, резервное копирование;.

Форма отчетности:

Отчет по лабораторной работе должен содержать следующие сведения:

- название и цель работы;
- модель информационной системы;
- преобразованная структура информационной системы;
- таблица угроз и средств защиты;
- выводы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

1.1 Теоретические сведения

Информационная система (ИС) — основной объект прикладной информатики. Несмотря на разнообразие ИС, все они имеют много общего.

Информационная система — Система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации. [ГОСТ 7.0 99].

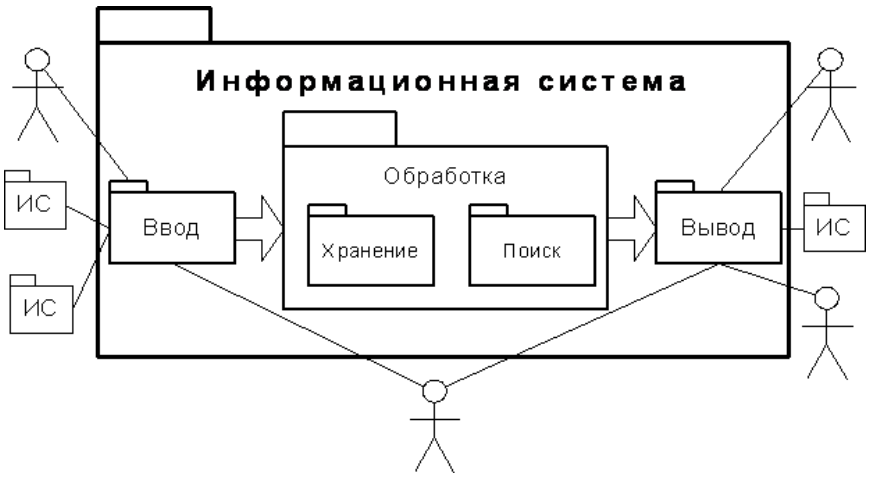

Рисунок 1 — Основные функции информационной системы

1.1.1 Функции информационной системы

1 Ввод информации (сбор информации, прием информации из других ИС).
2 Обработка информации (в частности, хранение и поиск информации).
3 Вывод информации (демонстрация ее человеку, передача в другие

ИС).Информационная система не обязательно использует компьютеры. Существуют многочисленные примеры некомпьютерных ИС: бухгалтерские учетные системы XVI – XX вв., карточные каталоги библиотек, любая книга, снабженная печатным справочным материалом, например, указателем.

Минимальная единица информации, хранимая и обрабатываемая информационной системой, называется *записью*. Многие операции, выполняемые информационными системами в процессе обработки информации, используют несколько записей одновременно.

Запись сама может иметь (и, как правило, имеет), внутреннюю структуру. Составляющие (элементы) записи обычно называются *полями.* Информационная система при обработке записи работает со всеми полями записи, хотя может создавать иллюзию того, что некоторые поля в обработке записи не участвуют.

Три функции информационной системы присутствуют в любой ИС, хотя могут иметь рудиментарные формы (например, в предметном указателе книги сбор информации и ее обработка были выполнены единственный раз, а вывод осуществляется перелистыванием книги ее читателем). Почти всякая отдельная программа может рассматриваться как информационная система. Например, текстовый процессор позволяет ввести информацию, он ее обрабатывает (хотя долговременным хранением информации для текстового процессора занимается операционная система), в текстовом процессоре возможет поиск информации, и уж конечно текстовый процессор умеет выво- дить информацию.

1.1.2 Предметная область

Информационные системы никогда не существую сами по себе. Они всегда связаны с какой-то деятельностью человека (организации): расчётом траектории ракеты, управлением движением самолётов, дозировкой лекарств, вводимых больному, расчётом заработной платы, учётом недвижимости, поиском веб-страниц, реконструкцией археологических объектов и др.

Деятельность, связанная непосредственно с информационными системами (и только с ними), редко бывает основной (если только организация не занята исключительно разработкой и/или сопровождением ИС). Информационная система всегда только обслуживает основную деятельность организации/человека.

Зачастую в организации эксплуатируется несколько информационных систем. Например, в библиотеке может работать библиотечная ИС (учёт читателей, электронный каталог, учёт книговыдачи и др.) и кадрово-бухгалтерская система (отдел кадров, учёт зарплаты).

Наличие тесной связи информационной системы и обслуживаемой ею деятельности позволяет говорить о предметной области ИС — объектах той деятельности, с которой эта ИС связана, и отношениях между этими объектами. Так, в библиотечной ИС объектами предметной области являются издания (книги, журналы, эстампы, музыкальные записи и др.), средствахранения изданий (хранилища и стеллажи), читатели, библиографы и др. А в кадрово-бухгалтерской информационной системе объектами предметной области будут сотрудники, должности, рабочее время, штатное расписание, премии и надбавки, налоги и пр.

Подсистемы

Каждая функция информационной системы может выполняться отдельным компонентом ИС. Такой компонент называется *подсистемой* или *модулем* (в зависимости от произвольно оцениваемой сложности или размера компонента). В небольших ИС подсис- тема может реализовать несколько функций; в больших и сложных ИС их функции детализируются (простейший пример — разделение функций хранения и обработки информации). Каждая такая детальная функция может реализовываться своей подсистемой; подсистемы могут реализовывать несколько различных детальных функций (относящихся, например, к одному из видов информации, обрабатываемой ИС). Например, подсистема расчета заработной платы в бухгалтерской ИС может реализовывать все 4 функции ИС, но по отношению только к некоторой части финансовой информации (используемой при расчете заработной платы, но не требующейся, например, для учета движения оборудования).

1.1.3 Обеспечения

Для того, чтобы подсистемы ИС могли реализовывать функции ИС, необходимы компоненты, согласованно используемые всеми или, по крайней мере, несколькими подсистемами.

Такие компоненты называются *обеспечениями* (или видами обеспечения). Различают по крайней мере пять обеспечений:

1 Аппаратное (компьютеры в той или иной комплектации; специфические для ИС периферийные устройства: сканеры, принтеры, синтезаторы звука, цифровые микрофоны, кассовые аппараты, устройства отображения информации и др.; устройства управления датчиками физических величин и считывания данных с них (например, счетчик яиц на конвейере птицефабрики); кабели и оборудование телекоммуникационных сетей; аппаратура электропитания и вентиляции и др.).

2 Программное (операционные системы; языки программирования, на которых выполняется разработка ИС; системы управления базами данных (СУБД); информационно-поисковые системы (ИПС);

библиотеки программных компонентов; серверное программное обеспечение, например, веб-сервер). В программное обеспечение информационных систем никогданевключаются средства их разработки (редакторы программных текстов, компиляторы и др.).

3 Лингвистическое (словари данных и другая метаинформация (информация об информации), искусственные языки, используемые в ИС — например, языки запросов к СУБД/ИПС, языки форматных преобразований; описания коммуникативных форматов и др.).

4 Информационное (полупостоянная информация, мало или совсем не изменяемая за время жизни ИС — нормативно-справочная информация (НСИ), — например, перечень районов города или список слов, не включаемых в словарь ИПС).Информационное и лингвистическое обеспечения иногда объединяют, включая лингвистическое обеспечение в информационное или наоборот.

5 Организационное (производственные роли, руководства пользователей и администраторов ИС).

6 Для реализации каждой функции информационной системы могут использоваться все или только часть обеспечений.

1.1.4 Жизненный цикл информационной системы

Информационные системы не существуют вечно — они создаются, работают (эксплуатируются) и замещаются другими информационными системами. Период от появления замысла информационной системы до её полного замещения другой ИС называется *жизненным циклом информационной системы*. Структуры жизненных циклов различных ИС бывают различны, о чаще всего они либо линейны — когда одна стадия жизненного цикла последовательно сменяет другую, — либо представляют собой спираль, когда стадии жизненного цикла сменяют друг друга, неоднократно повторяя некоторую последовательность стадий — каждый раз для более развитой версии информационной системы.

Линейный жизненный цикл информационной системы

Рисунок 2 — Линейный жизненный цикл информационной системыЛинейный жизненный цикл

информационной системы состоит из трёх стадий:

1 Разработка (создание, производство)

2 Эксплуатация и сопровождение (использование и доработка)

3 Замещение другой информационной системой (с сохранением накопленных данных)

Линейный жизненный цикл в настоящее время характерен для военных и других информационных систем, связанных с использованием определённого оборудования (например, мобильных телефонов; с выработкой ресурса оборудования ИС замещается вместе с оборудованием) или высокими требованиями к качеству ИС (управление воздушным движением, обеспечение жизнедеятельности пациента в больнице и др.).

Существенным элементом линейного жизненного цикла информационной системы является так называемое *сопровождение системы*. Процесс сопровождения включает две разновидности мероприятий:

1 Администрирование — мероприятия, направленные на поддержание приемлемых эксплуатационных характеристик ИС (используемые ресурсы, надёжность и др.),

2 Сопровождение разработки — мероприятия, имеющие целью изменение характеристик ИС (прежде всего, обнаружение и исправление ошибок; но также и модификация ИС для решения новых задач, не предусмотренных при её разработке, или для обеспечения возможности эксплуатации ИС в условиях, которые также не были предусмотрены, например, на иной аппаратуре).

Сопровождение разработки при линейном жизненном цикле информационной системы — аналог авторского надзора в строительстве— может выполняться как разработчиками, так и эксплуатационным персоналом и/или третьими организациями.

1.1.5 Спиральный жизненный цикл

Большинству современных информационных систем присущ спиральный жизненный цикл. В спиральном жизненном цикле информационной системы эксплуатация ИС может быть не связана с процессом сопровождения разработки (однако от администрирования всё равно никуда не деться). Ошибки, обнаруженные в процессе эксплуатации, и требования изменений, которые необходимо внести в информационную систему, фиксируются в фазе оценки информационной системы и поступают к разработчикам, которые через определённые интервалы времени выпускают новый вариант информационной системы, называемый *версией* (редакцией, релизом и т.п.). С получением очередной версии ИС эксплуатационный персонал замещает ею её

предыдущую версию. В реальности фазы эксплуатации, оценки и разработки могут совмещаться во времени.

Рисунок 3 — Спиральный жизненный цикл информационной системы

Использование информационных систем со спиральным жизненным циклом позволяет:

во-первых, сократить время от начала разработки до начала эксплуатации ИС (за счёт ограничения функциональности первой версии ИС); *во-вторых,* относительно быстро (с задержкой, равной времени выпуска очередной версии, которое может быть равным, например, даже двум неделям) реагировать на обнаруживаемые ошибки, изменяющиеся требования пользователей и изменяющиеся условия эксплуатации информационной системы.

С каждой формой жизненного цикла информационной системы связан определённый тип процесса её разработки. Линейному жизненному циклу соответствует так называемый *«водопадный» процесс* («сразу и целиком»), а спиральному жизненному циклу — разнообразные итерационные (пошаговые) процессы разработки ИС.

В литературе (да и в жизни) для информационных систем со спиральным жизненным циклом понятия жизненного цикла и процесса разработки зачастую отождествляются. Причина такого отождествления понятна — в этом случае разработка ведётся параллельно эксплуатации ИС, в течение всего её жизненного цикла.

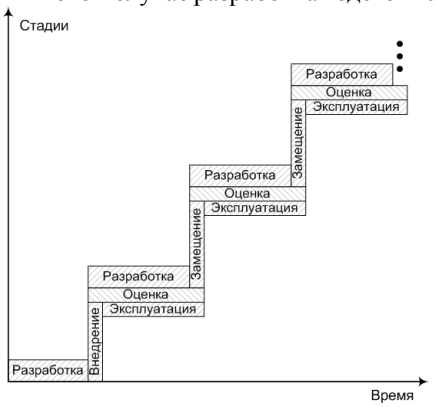

Рисунок 4 — Спиральный жизненный цикл как смена версий

Рекомендуемые источники

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М., 2009, 50 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=173886 2.
2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М., 2008, 31 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=129018 3.
3. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2014, 106 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=183918 4.
4. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства

обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. М., 2014, 58 с. [Электронный ре- сурс].http://protect.gost.ru/document.aspx?control=7&id=18359

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.
2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.
3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

4. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)
5. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки

1. Понятие информационной системы.
2. Функции информационной системы.
3. Жизненный цикл информационной системы.
4. ГОСТ Р ИСО/МЭК ТО 18044-2007
5. ГОСТ Р ИСО/МЭК 27001-2006
6. ГОСТ Р ИСО/МЭК 27003-2012
7. ГОСТ Р ИСО/МЭК 27002-2012

Лабораторная работа №2 Анализ и управление рисками информационной системы компании

Цель работы: практическое изучение анализа рисков информационной системы на основе программного продукта ГРИФ 2006 из состава Digital Security Office.

Задание:

Порядок выполнения:

1. **Начало работы с программой**

Запустите ярлык «ГРИФ 2006» на рабочем столе. Для входа в систему под именем пользователя «user» используйте пароль «user».В окне «Алгоритм анализа рисков» (рисунок 1) выберите пункт «Анализ модели информационных потоков», создайте новый проект.

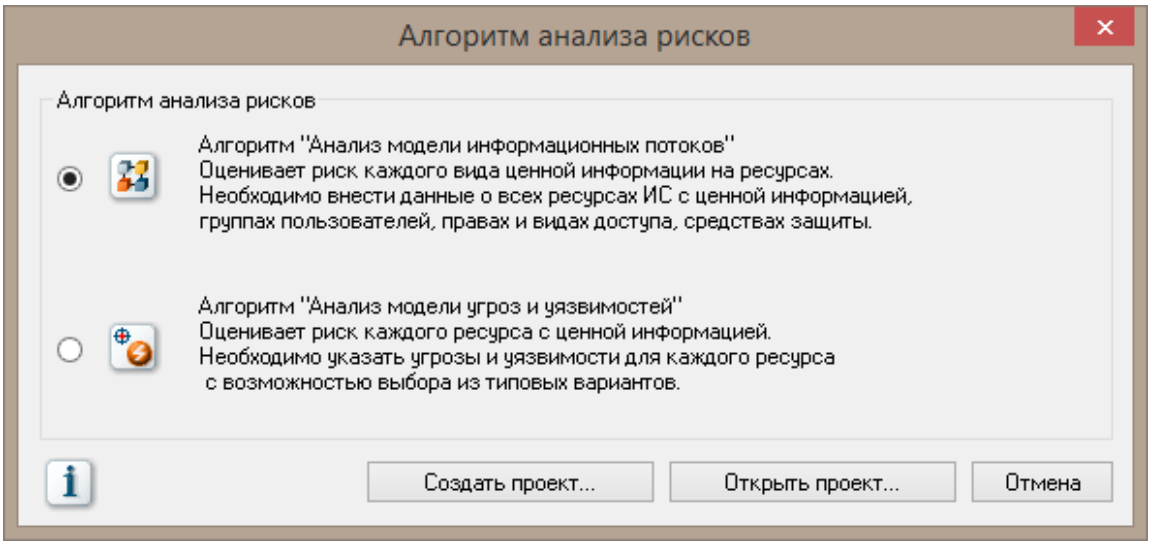

Рисунок 1 – Создание проекта

2. Модель информационных потоков

Шаг 1. На первом этапе работы с программой пользователь вносит все объекты своей информационной системы: отделы, ресурсы (специфичными объектами данной модели являются сетевые группы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

Шаг 2. Далее пользователю необходимо проставить связи, т.е. определить к каким отделам и сетевым группам относятся ресурсы, какая информация хранится на ресурсе, и какие группы пользователей имеют к ней доступ. Также пользователь системы указывает средства защиты ресурса и информации.

Шаг 3. На завершающем этапе пользователь отвечает на список вопросов по политике безопасности, реализованной в системе, что позволяет оценить реальный уровень защищенности системы и детализировать оценки рисков.

2.1 Модель информационной системы

Для начала работы необходимо иметь описание системы:

Информационная система Компании состоит из одного отдела – бухгалтерии. Имеются сервер и рабочая станция, которые физически связаны между собой. На сервере хранятся два вида информации: бухгалтерский отчет и база клиентов; на рабочей станции – база данных наименований товаров с описанием. В компании есть три сотрудника: финансовый директор, главный бухгалтер, бухгалтер. К бухгалтерскому учету на сервере локальный доступ имеет главный бухгалтер, к базе клиентов удаленный доступ имеют бухгалтер (с рабочей станции через коммутатор) и финансовый директор. При чем финансовый директор имеет удаленный доступ через Интернет. К базе данных наименований товаров с описанием на рабочей станции локальный доступ имеет бухгалтер.

Для описания информационной системы существуют такие виды объектов, как отделы, сетевые группы, ресурсы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы (Рисунок 2).

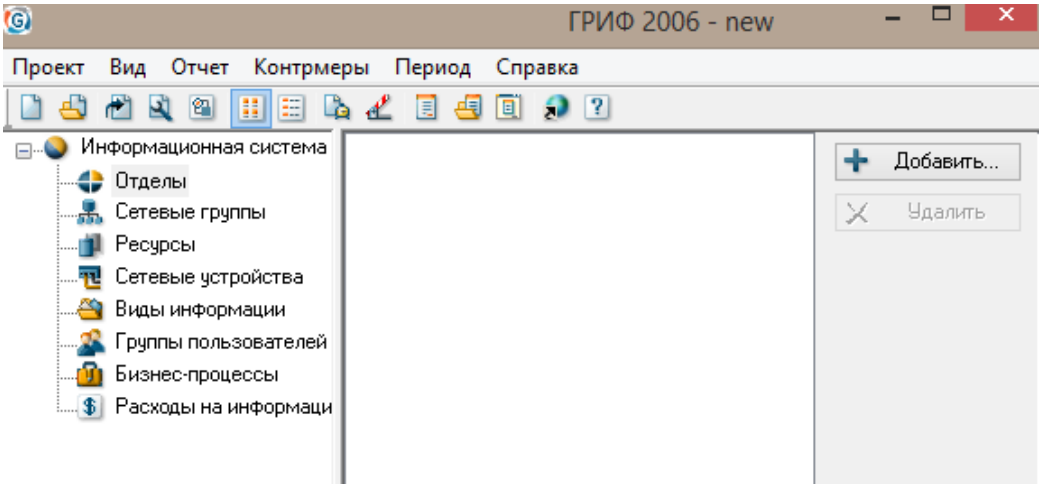

Рисунок 2 – Основное окно программы

Внесем входные данные. Так как, информационная система Компании состоит из одного отдела – бухгалтерии. В отделе имеется одна сетевая группа.

Добавьте отдел «Бухгалтерия» и одноименную сетевую группу (Рисунок 3).

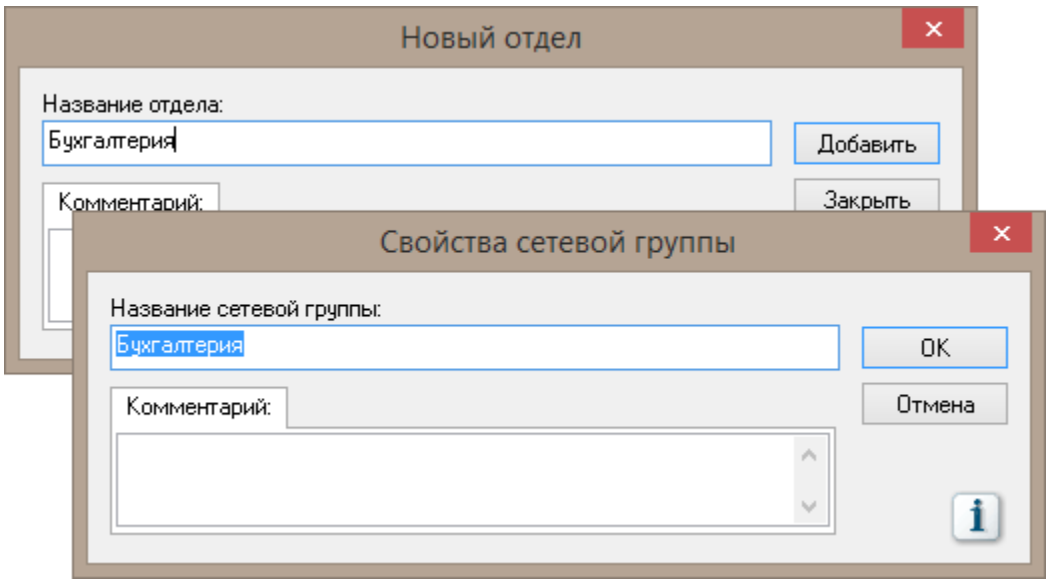

Рисунок 3 – Добавление нового отдела и сетевой группы

Информационная система содержит два ресурса: сервер и рабочую станцию, которые физически связаны между собой (находятся в одной сетевой группе).

Добавьте ресурсы «Сервер» и «Рабочая станция», указав тип ресурса (сервер, рабочая станция, мобильный компьютер, твердая копия, веб-сервер), сетевую группу и отдел, к которым принадлежит ресурс (Рисунок 4).

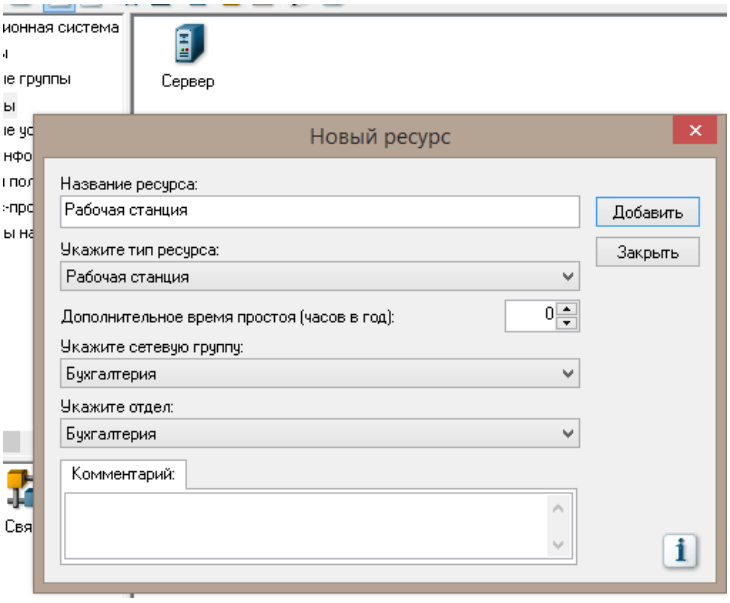

Рисунок 4 – Добавление нового сетевого ресурса

На сервере хранятся два вида информации: бухгалтерский отчет и база клиентов; на рабочей станции – база данных наименований товаров с описанием. Добавьте эти три вида информации аналогичным образом.

Рассмотрим трех сотрудников, каждый из которых отнесем к отдельной группе пользователей. Создайте группы пользователей: главный бухгалтер, бухгалтер и финансовый директор. При чем для финансового директора укажите класс группы пользователей «Авторизованные пользователи из Интернет» (так как у него должен быть удаленный доступ к базе клиентов компании), а для бухгалтеров – «Пользователи».

В зависимости от выбора класса будут предложены средства защиты рабочего места группы пользователей. Средства защиты клиентского места групп авторизованных Интернет-пользователей (здесь - финансовый директор) оценить невозможно, т.к. неизвестно, откуда будут осуществлять доступ пользователи этой группы. Для клиентского места бухгалтера укажите следующие средства защиты: контроль доступа в помещение, где расположен ресурс (дверь с замком, видео наблюдение); средства антивирусной защиты (антивирусный монитор); отсутствие возможности подключения внешних носителей; персональный межсетевой экран; система криптозащиты электронной почты. То же самое проделайте и для клиентского места главного бухгалтера, отметьте разрешение доступа в Интернет.

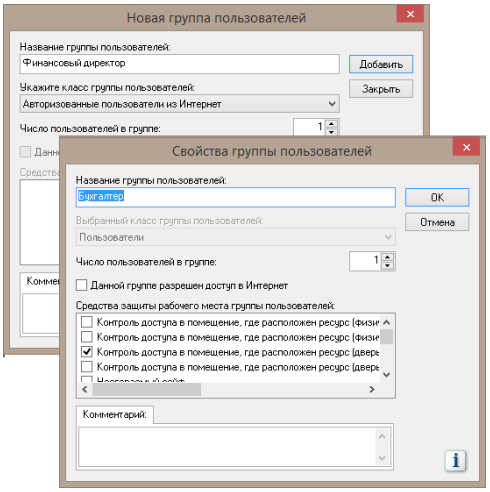

Рисунок 5 – Добавление новой группы пользователей

К информации «бухгалтерский учет» на сервере локальный доступ имеет группа пользователей «главный бухгалтер».

К информации «база клиентов» на сервере удаленный доступ имеют группы пользователей «бухгалтер» (с рабочей станции через коммутатор) и «финансовый директор» (через глобальную сеть Интернет, как уже было указано).

К информации «база данных наименований товаров с описанием» на рабочей станции локальный доступ имеет группа пользователей «бухгалтер».

Соответственно, для полного описания информационной системы необходимо добавить сетевое устройство типа «коммутатор».

2.2 Связи

После добавления всех объектов в информационную систему, пользователю необходимо проставить связи, т.е. определить к каким отделам и сетевым группам относятся ресурсы, какая информация хранится на ресурсе и какие группы пользователей имеют к ней доступ. Также, пользователь системы указывает средства защиты ресурса и информации.

В левом нижнем поле основного окна выберите «Связи».

Для добавления к ресурсу «Сервер» двух видов информации (как указано выше) «Бухгалтерский отчет» и «База клиентов» необходимо в вкладке «Виды информации» кнопкой «Добавить» вызвать окно добавления вида информации, в котором в выпадающем меню выбрать требуемые пункты.

После выбора вида информации станет доступно поле «Ущерб по угрозам». Установите ущерб по угрозе «Конфиденциальность» - 100 у.е. в год, по угрозе «Целостность» - 100 у.е. в год, по угрозе «Доступность» - 1 у.е. в час для обоих видов информации (Рисунок 6).

В случае, если единицы измерения ущерба по угрозам отличны от у.е., откройте справку, найдите каким образом выбрать другие единицы измерения.

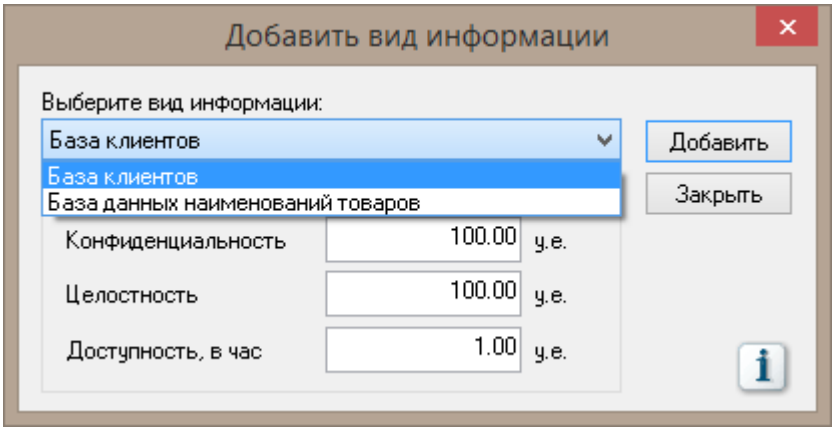

Рисунок 6 – Добавление вида информации к ресурсу

Проделайте аналогичные действия для ресурса «Рабочая станция» (вид информации – «База данных наименований товаров»; ущерб по угрозам в точности такой же, как и у других видов).

Перейдите на вкладку «Группы пользователей»

Укажите группы пользователей и их права на конкретный вид информации в соответствии с таблицей 1. (Пример см. на рисунке 7)

Таблица 1 - Вид и права доступа групп пользователей к информации, наличие соединения через VPN, количество человек в группе

	Вид доступа	Права доступа	Наличие VPN-соединения	Количество человек в группе
Главный бухгалтер / бухгалтерский отчет	локальный	чтение, запись, удаление	нет	1
Бухгалтер / база клиентов	удаленный	чтение	есть	1
Финансовый директор / база клиентов	удаленный	чтение, запись	есть	1
Бухгалтер / база данных наименований товаров	локальный	чтение, запись, удаление	нет	1

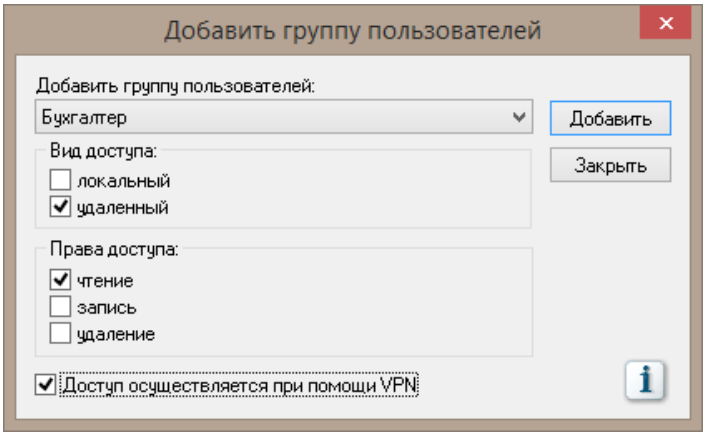

Рисунок 7 – Добавление группы пользователей и их права на конкретный вид информации

Во вкладке «Каналы связи» укажите, что группа пользователей «бухгалтер» имеет доступ к ресурсу «Сервер» через сетевое устройство «Коммутатор».

Чтобы указать средства защиты ресурса, перейдите на вкладку «Средства защиты», нажмите кнопку «Изменить» (Рисунок 8) и укажите для ресурса «Сервер» следующие пункты: контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещение); отсутствие возможности подключения внешних носителей; межсетевой экран; обманная система; система антивирусной защиты на сервере; аппаратная система контроля целостности. Для ресурса «Рабочая станция» задайте средства защиты из шаблона (необходимо задать: контроль доступа в помещение, где расположен ресурс (дверь с замком, видеонаблюдение); средства антивирусной защиты (антивирусный монитор); отсутствие возможности подключения внешних носителей; персональный межсетевой экран; система криптозащиты электронной почты). Для этого в окне выбора шаблона выберите группу пользователей «Бухгалтер» (Рисунок 9).

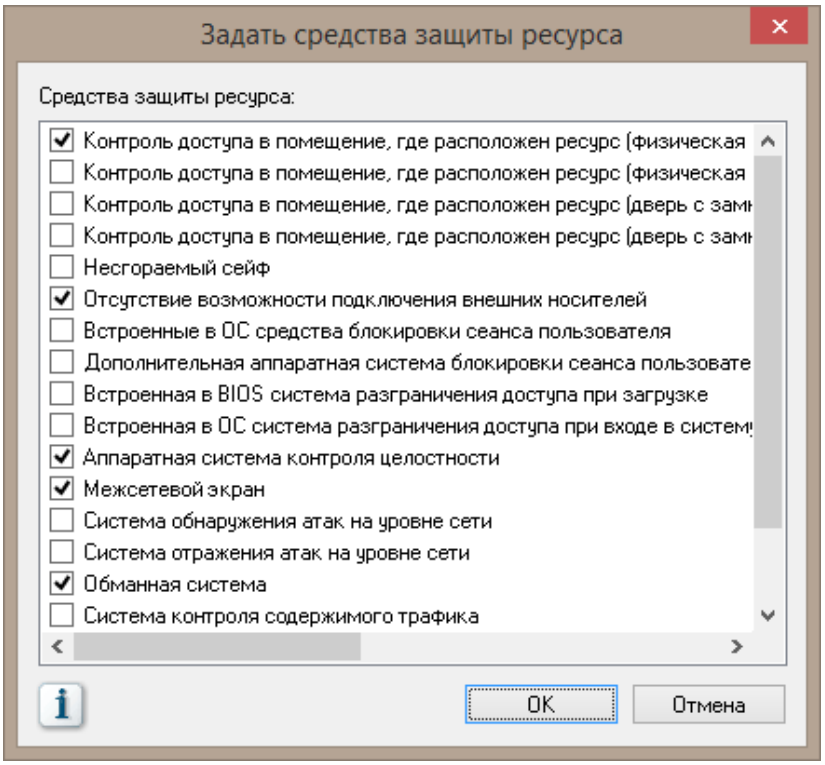

Рисунок 8 – Задание средства защиты ресурса

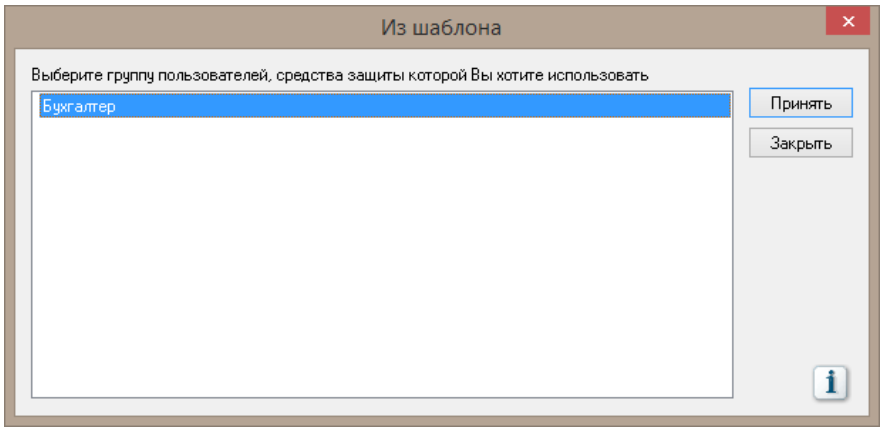

Рисунок 9 – Выбор средства защиты из шаблона

В последней вкладке необходимо указать средства защиты для каждого вида информации. Для вида информации «Бухгалтерский учет» отметьте все средства защиты, кроме «Дополнительная программно-аппаратная система контроля доступа» (Рисунок 10).

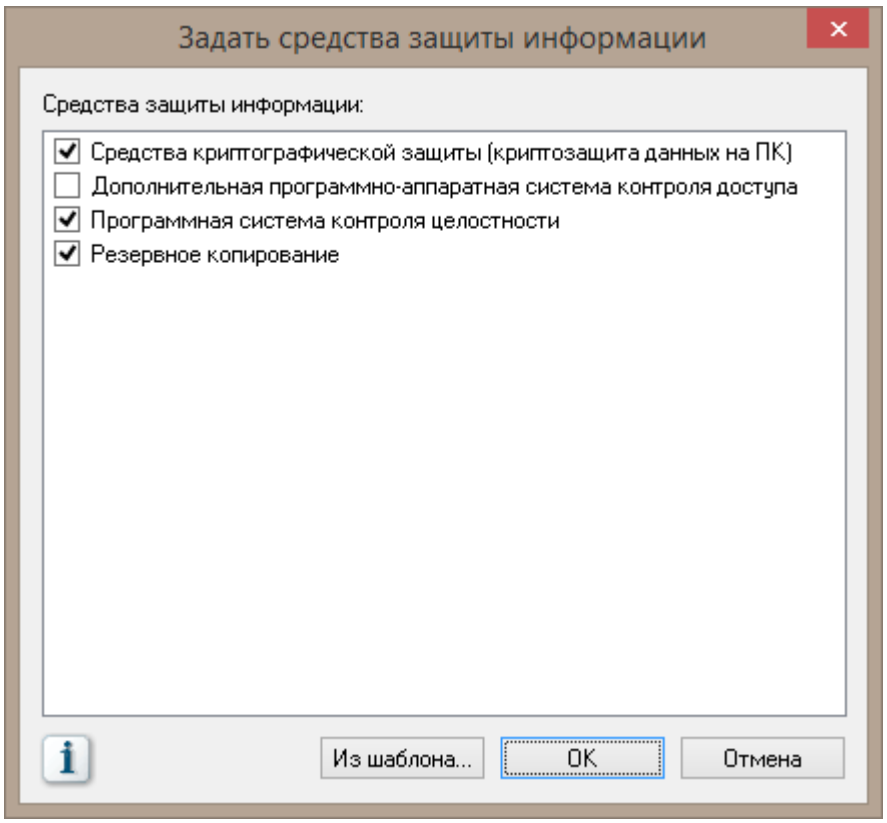

Рисунок 10 – Выбор средства защиты информации

Для вида информации «База клиентов» средств защиты информации нет.

Для вида информации «База данных наименований товаров» укажите пункты «Резервное копирование» и «программная система контроля целостности».

Политика безопасности

Так как модель «Информационных потоков» не может учесть организационные меры, связанные с поведением сотрудников организации, существует раздел «Политика безопасности».

В нем пользователю необходимо ответить на ряд вопросов, ответы на вопросы влияют на веса средств защиты и изменяют риск реализации информационной безопасности.

Разделы «Политики безопасности» (Рисунок 11):

- Политика безопасности;
- Организационные меры;
- Безопасность персонала;
- Физическая безопасность;

– Управление коммуникациями и процессами;
– Контроль доступа;
– Разработка и сопровождение;
– Непрерывность ведения бизнеса;
– Соответствие системы требованиям.

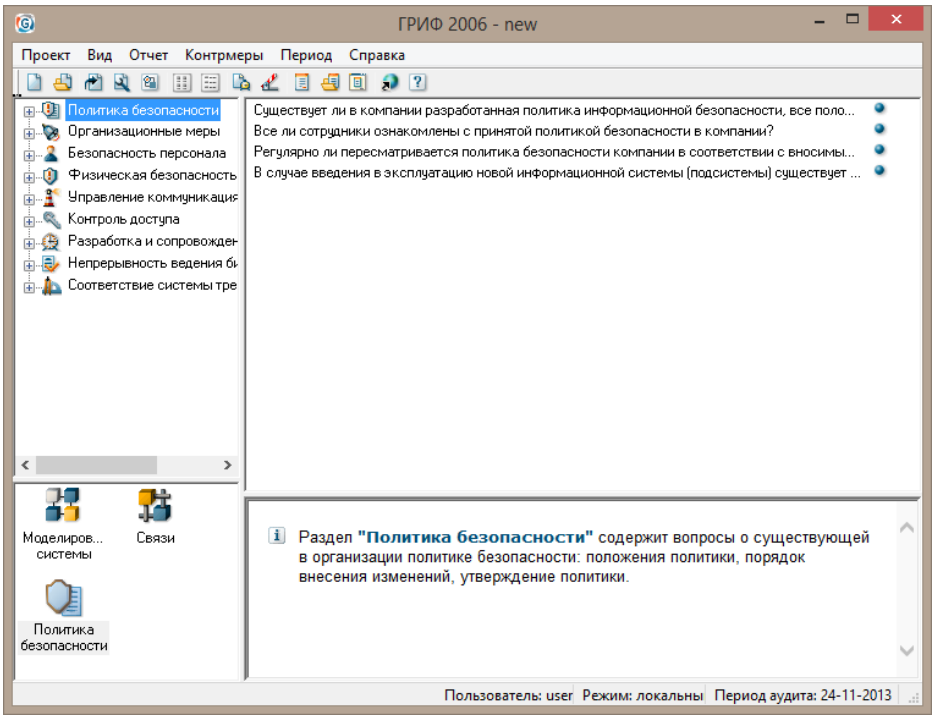

Рисунок 11 – Раздел «Политика безопасности»

Примеры вопросов.

Вопрос 1:

Существует ли в компании разработанная политика информационной безопасности, все положения которой на практике внедрены в информационную систему?

Варианты ответов:

— Да
— Нет
— Положения политики внедрены частично

Вопрос 2:

Может ли раскрытие какой-либо информации принести существенную выгоду посторонним лицам, заинтересованным организациям и т. п.?

Варианты ответов:

— Да
— Нет

Ответьте на вопросы по собственному усмотрению.

2.3 Контрмеры

После выполнения всех этапов, на выходе пользователь получает полную сформированную модель информационной системы с точки зрения информационной безопасности, что позволяет перейти к программному анализу введенных данных для комплексной оценки рисков, а также внедрению контрмер.

Для перехода в окно управления рисками, в главном меню выберите пункт «Контрмеры» и из выпадающего списка нажмите «Управление рисками» (Рисунок 12).

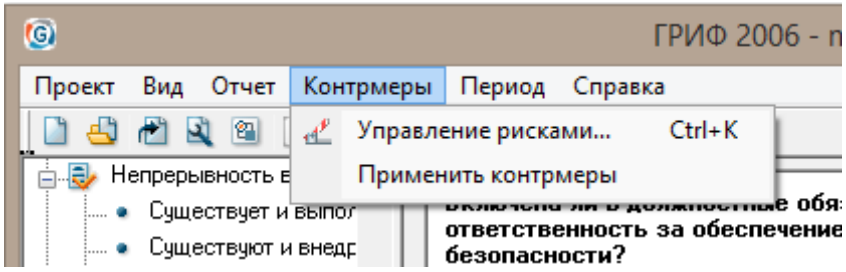

Рисунок 12 –Меню «Контрмеры»

После чего появится окно «Управление рисками», в нем содержится информация по каждому ресурсу системы, средствах защиты каждого ресурса отдельно, а также сведенья о пользователях (Рисунок 13).

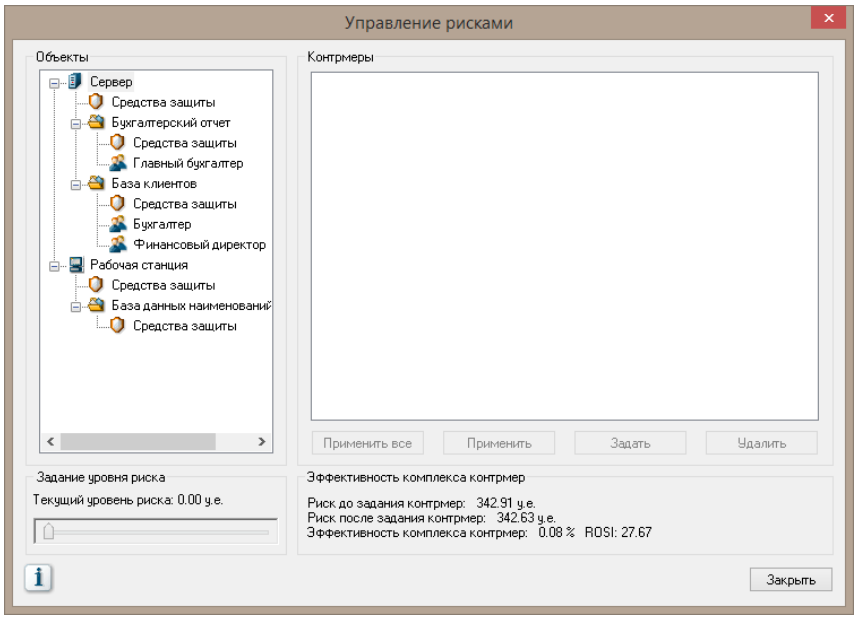

Рисунок 13 – «Управление рисками»

В нижней части окна расположены регулятор уровня риска «Задание уровня риска» (по умолчанию он установлен в 0) и информация об эффективности контрмер для всей системы.

Регулятор уровня риска позволяет отфильтровать объекты системы по значимости, например по умолчанию он установлен в 0.00 у.е., это означает что в поле

«Объекты» буду показаны все объекты, уровень риска которых превышает данный порог.

Передвинув регулятор вправо, определите какой уровень риска не превышает ресурс «Рабочая станция».

В поле «Эффективность комплекса контрмер» показан суммарный риск всей системы.

Для внедрения контрмер выберите интересующий вас ресурс, в рамках ресурса будет показано, какие средства защиты не используются для защиты ресурса, какой вид информации использует данный ресурс и какие средства защиты еще не применены к данному виду информации, а также какая группа пользователей работает с данной информацией.

Выберите одно из предложенных средств защиты, нажмите кнопку «Задать», откроется окно «Новая контрмера» (Рисунок 14)

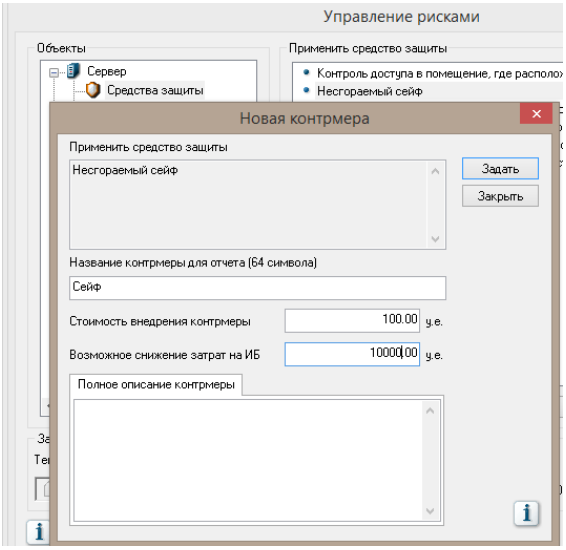

Рисунок 14 – Задание контрмеры

Заполните необходимы поля в соответствии с Рисунком 14, нажмите «Задать», контрмера будет учитываться при расчете риска в окне «Эффективность комплекса контрмер» (Рисунок 15). Примите еще несколько контрмер.

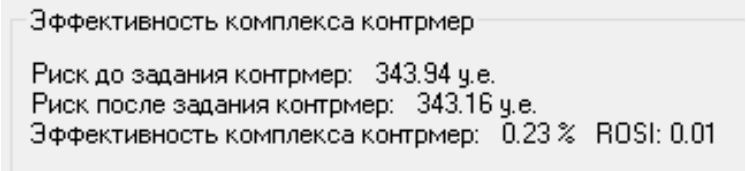

Рисунок 15 – Риск после задания контрмеры

Внедрение контрмеры, напрямую снижает уровень риска реализации угроз, чем больше будет применено контрмер к системе, тем ниже будет показатель риска.

Заданные контрмеры подсвечиваются оранжевым кругом, после применения контрмеры, она пропадет из списка, а риск информационной системы обновится.

Вы можете принять все контрмеры, или только некоторые, исходя из необходимости и возможности их внедрения в рассматриваемую вами конкретную систему.

Отчет

Результатом

работы системы ГРИФ является отчет, содержащий расчеты затрат компании на ИБ, на контрмеры, вероятности реализации рисков в общем и по отделам и другую информацию, представленную в виде обобщающих диаграмм, графиков и таблиц.

Создайте отчет, для чего в главном меню системы гриф выберите пункт «Отчет» и нажмите «Создать отчет…».

Появится окно конфигурации отчета, в нем пользователь выбирает, какая информация будет выведена в отчете и в каком виде (рисунок 16).

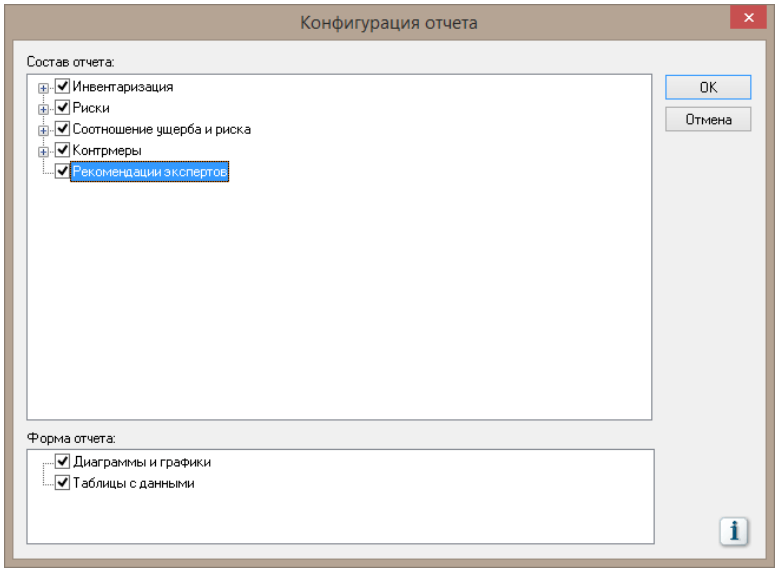

Рисунок 16 – Конфигурация отчета

Ознакомьтесь с содержанием отчета.

3. Модель угроз и уязвимостей

Шаг 1. На первом этапе работы с продуктом пользователь вносит объекты своей информационной системы: отделы, ресурсы (специфичными объектами для данной модели: угрозы информационной системы, уязвимости, через которые реализуются угрозы).

Шаг 2. Далее пользователю необходимо проставить связи, т.е. определить к каким отделам относятся ресурсы, какие угрозы действуют на ресурс и через какие уязвимости они реализуются.

С данной моделью ознакомьтесь самостоятельно.

Форма отчетности:

Отчет по лабораторной работе должен содержать следующие сведения:

- название и цель работы;
- модель информационной системы;
- преобразованная структура информационной системы;
- таблица угроз и средств защиты;

- выводы.

Рекомендуемые источники

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М., 2009, 50 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=173886 2.
2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М., 2008, 31 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=129018 3.
3. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2014, 106 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=183918 4.
4. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. М., 2014, 58 с. [Электронный ре- сурс].http://protect.gost.ru/document.aspx?control=7&id=18359

Основная литература

6. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.
7. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.
8. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

9. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)
10. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки

1. Что представляет собой система ГРИФ и для чего она предназначена?
2. Что понимается под характеристиками группы пользователей?
3. Что такое эффективность средства защиты?
4. С какой целью создан раздел контрмер?
5. Опишите пошагово работу с моделью информационных потоков.
6. Почему для класса группы авторизованных Интернет-пользователей система ГРИФ не предлагает никакие средства защиты рабочего места?
7. По каким угрозам оценивается ущерб в изученной системе?Как повлияет на веса средств защиты ответ «Положения политики внедрены частично» на первый вопрос раздела о политике безопасности?
8. Опишите пошагово работу с моделью угроз и уязвимостей.
9. На какие категории система ГРИФ делит угрозы?

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

ОС Windows 7 Professional
Microsoft Office 2007 Russian Academic OPEN No Level
Антивирусное программное обеспечение Kaspersky Security.

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Вид занятия (*Лк, Лр , кр)*	***Наименование аудитории***	***Перечень основного оборудования***	***№ Лр***
1	**3**	**4**	**5**
Лк	Лаборатория технических средств защиты информации	Оборудование Интерактивная доска Smart Board X885ix со встроенным проектором UX60	№ 1.1 -3.2
ЛР	Лаборатория технических средств защиты информации	Оборудование 16-ПК i5-2500/H67/4Gb/500Gb (монитор TFT19 Samsung E1920NR); интерактивная доска Smart Board X885ix со встроенным проектором UX60	№ 1-5
СР	Читальный зал №1	Оборудование 10 ПК i5-2500/H67/4Gb(монитор TFT19 Samsung); принтер HP LaserJet P2055D	-

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-6	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	**1.** Система управления информационной безопасностью.	1.1. Анализ объекта защиты.	Вопросы к зачету
ОПК-4	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности		1.2 Модель угроз и модель нарушителя.	Вопросы к зачету
			1.3 Оценка рисков информационной безопасности	Вопросы к зачету
			1.4 Политика информационной безопасности	Вопросы к зачету
			1.5 Управление инцидентами информационной безопасности.	Вопросы к зачету

2. Вопросы к зачету

№ п/п	Компетенции		ВОПРОСЫ К ЗАЧЕТУ	№ и наименование раздела
	Код	Определение		
1	2	3	4	5
1.	ПК-6	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных,	**1.** Цель и этапы анализа объектов защиты.	**1.** Система управления информационной безопасностью
			2. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем.	
			3. Методика определения актуальных угроз (ФСТЭК).	

		профессиональных и этических позиций		
2.	ОПК-4	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности	**4.** Упрощённая модель классификации субъектов.	
			5. Основные положения инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации.	
			6. Основные положения инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации.	
			7. Приведите примеры источников информации об инцидентах информационной безопасности.	
			8. Перечислите аспекты анализа инцидентов информационной безопасности, направленные на совершенствование системы управления информационной безопасностью.	
			9. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности.	
			10. Формальное описание структуры информационной системы.	
			11. Составление модели угроз информационной системе.	
			12. Формирование требований к системе защиты информации.	
			13. Формирование регламента действий при возникновении нештатных ситуаций	
			14. Формирование требований к политике информационной безопасности..	

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать ПК-6: – принципы и методы противодействия	**зачтено**	Студент демонстрирует сформированность дисциплинарных компетенций на итоговом уровне, обнаруживает всестороннее,

несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; – способы формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций. ОПК-4: основные стандарты ИБ **Уметь** ПК-6: – настраивать и эксплуатировать программные средства; – разрабатывать политику информационной безопасности; ОПК-4: – решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности; **Владеть** ПК-6: – профессиональной терминологией; навыками формирования суждений о значении и последствиях своей профессиональной деятельности с учетом		систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
	не зачтено	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже базового, проявляется недостаточность знаний, умений, навыков. Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

социальных, профессиональных и этических позиций**.** ОПК-4: – навыками применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности.		

4. Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

4.1 Вопросы на самоподготовку

1. Формальное описание структуры информационной системы.
2. Составление модели угроз информационной системе.
3. Формирование требований к системе защиты информации.
4. Формирование требований к политике информационной безопасности.
5. Формирование регламента действий при возникновении нештатных ситуаций.

Приложение 2

АННОТАЦИЯ
рабочей программы дисциплины
Управление информационной безопасностью

1. Цель и задачи дисциплины

Целью дисциплины является овладение основными принципами управления уровнем ин формационной безопасности защищаемых ресурсов организации.

Задачами изучения дисциплины являются:

- Получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.
- Получение студентами умений и навыков по построению моделей угроз и нарушителей и по оценке рисков информационной безопасности в организации.
- Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: Лк.-24 час., ЛР-24 час.; СР 60 час.

Общая трудоемкость дисциплины составляет 108 часов, 3 зачетных единиц.

2.2 Основные разделы дисциплины:

1. Система управления информационной безопасностью.

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-6 Способностью формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций

ОПК-4 Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности

4. Вид промежуточной аттестации: зачет.

Приложение 3

Протокол о дополнениях и изменениях в рабочей программе
на 20___-20___ учебный год

1. В рабочую программу по дисциплине вносятся следующие дополнения:
_____
_____

2. В рабочую программу по дисциплине вносятся следующие изменения:

_____
_____
_____

Протокол заседания кафедры №____ от «___» _____ 20 __ __ г.,
(разработчик)

Заведующий кафедрой _____ _____
(подпись) *(Ф.И.О.)*

Приложение 4

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-6	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	**1.** Система управления информационной безопасностью.	1.1. Анализ объекта защиты.	Отчет по ЛР
ОПК-4	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности		1.2 Модель угроз и модель нарушителя.	Отчет по ЛР
			1.3 Оценка рисков информационной безопасности	Отчет по ЛР
			1.4 Политика информационной безопасности	Отчет по ЛР
			1.5 Управление инцидентами информационной безопасности.	Отчет по ЛР

2. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать ПК-6: – принципы и методы противодействия	**зачтено**	Студент демонстрирует сформированность дисциплинарных компетенций на итоговом уровне, обнаруживает всестороннее,

несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; – способы формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций. ОПК-4: основные стандарты ИБ **Уметь** ПК-6: – настраивать и эксплуатировать программные средства; – разрабатывать политику информационной безопасности; ОПК-4: – решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности; **Владеть** ПК-6: – профессиональной терминологией; навыками формирования суждений о значении и последствиях своей профессиональной деятельности с учетом		систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
	Не зачтено	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже базового, проявляется недостаточность знаний, умений, навыков. Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

социальных, профессиональных и этических позиций**.** ОПК-4: – навыками применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности.		

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.02 Прикладная математика и информатика от «12» марта 2015 г. №228

для набора 2015 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «13» июля 2015 г. №475

для набора 2016 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06»июня 2016 г. №429

для набора 2017 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06» марта 2017 г. №125

для набора 2018 года и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «12» марта 2018 г. №130

Программу составил:

Сташок О.В. к.т.н, доцент каф. математики и физики _____

Рабочая программа рассмотрена и утверждена на заседании кафедры математики и физики

от «21» ноября 2018 г., протокол № 3

Заведующий кафедрой
Математики и физики _____ О.И.Медведева

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой МиФ _____ О.И Медведева

Директор библиотеки _____ Т.Ф.Сотник

Рабочая программа одобрена методической комиссией ЕН факультета

от «20» декабря 2018 г., протокол № 4
Председатель методической комиссии факультета _____ М.А. Варданян

СОГЛАСОВАНО:
Начальник
учебно-методического управления _____ Г.П. Нежевец

Регистрационный №_____

(методический отдел)