

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное автономное образовательное учреждение  
высшего образования  
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

---

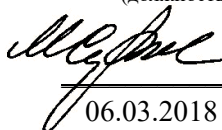
Кафедра №44

«УТВЕРЖДАЮ»

Руководитель направления

д.т.н., проф.

(должность, уч. степень, звание)

  
М.Б. Сергеев  
06.03.2018

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Технологии информационной безопасности вычислительных систем»  
(Название дисциплины)

Код направления	09.03.01
Наименование на- правления	Информатика и вычислительная техника
Наименование на- правленности	Вычислительные машины, комплексы, системы и сети
Форма обучения	заочная

Санкт-Петербург 2018г.

## Лист согласования рабочей программы дисциплины

Программу составил(а)

доц., к.т.н.

  
06.03.2018

В.В. Балберин

Программа одобрена на заседании кафедры № 44

06.03.2018, протокол № 6-17/18

Заведующий кафедрой № 44

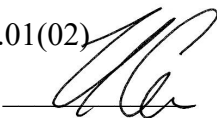
д.т.н., проф.

  
06.03.2018

М.Б. Сергеев

Ответственный за ОП 09.03.01(02)

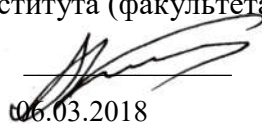
доц., к.т.н., доц.

  
06.03.2018

Н.В. Соловьев

Заместитель директора института (факультета) № 4 по методической работе

доц., к.т.н., доц.

  
06.03.2018

А.А. Ключарев

## Аннотация

Дисциплина «Технологии информационной безопасности вычислительных систем» входит в вариативную часть образовательной программы подготовки студентов по направлению «09.03.01 «Информатика и вычислительная техника» направленность «Вычислительные машины, комплексы, системы и сети». Дисциплина реализуется кафедрой №44

Дисциплина нацелена на формирование у выпускника

общефессиональных компетенций:

ОПК-5 «способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности».

Содержание дисциплины охватывает круг вопросов, связанных с проектированием и эксплуатацией безопасных вычислительных систем и корпоративных сетей.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский».

## 1. Перечень планируемых результатов обучения по дисциплине

### 1.1. Цели преподавания дисциплины

Получение студентами необходимых знаний и навыков в области проектирования, и эксплуатации безопасных вычислительных систем и корпоративных сетей различного назначения.

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

В результате освоения дисциплины студент должен обладать следующими компетенциями: ОПК-5 «способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности»:

знать - методологию построения безопасных вычислительных систем и сетей, нормативно-правовые документы, регламентирующие вопросы обеспечения безопасности корпоративных сетей,

уметь - анализировать угрозы безопасности конкретной вычислительной системы или корпоративной сети,

владеть навыками – по разработке и реализации предложений по созданию системы защиты для конкретных вычислительных систем и корпоративных сетей,

иметь опыт деятельности – по проведению аудита безопасности вычислительных систем и сетей.

## 2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных студентами при изучении следующих дисциплин:

- Сети ЭВМ и телекоммуникации
- Технология разработки открытого программного обеспечения.

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при подготовке выпускной квалификационной работы бакалавра.

## 3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№10
<b>Общая трудоемкость дисциплины, ЗЕ/(час)</b>	2/ 72	2/ 72
<i>Аудиторные занятия</i> , всего час., <i>В том числе</i>	24	24
лекции (Л), (час)	12	12
Практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	12	12

курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)		
<b>Самостоятельная работа</b> , всего (час)	48	48
<b>Вид промежуточной аттестации:</b> зачет, экзамен, дифференцированный зачет ( <b>Зачет. Экз. Дифф. зач</b> )	Зачет	Зачет

#### 4. Содержание дисциплины

##### 4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 10					
Раздел 1. Основы информационной безопасности	5		4		20
Раздел 2. Обеспечение безопасности вычислительных систем и сетей	7		8		28
Итого в семестре:	12		12		48
Итого:	12	0	12	0	48

##### 4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	<p>Тема 1.1. Введение в информационную безопасность. Сетевая инфраструктура организации и ее компоненты. Создание модели сетевой инфраструктуры. Методология безопасности. Анализ рисков и оборонительные модели.</p> <p>Тема 1.2 Организация информационной безопасности. Роли и ответственности. Управление жизненным циклом безопасности. Аудит безопасности. Службы мониторинга безопасности. Уровни защиты информационных систем. Политика информационной безопасности. Системы защиты элементов сетевой инфраструктуры.</p> <p>Тема 1.3. Аппаратно-программное обеспечение информационной безопасности. Криптография в обеспечении информационной безопасности. Конфиденциальность информации. Алгоритмы шифрования. Обнаружение нарушения целостности. Аутентичность информации. Инфраструктура открытых ключей. Модели доверия. Доверие к сертификатам. Цикл жизни цифрового сертификата.</p>
2	<p>Тема 2.1. Атаки на информационные системы и их отражение. Фазы вторжения. Атаки на сеть и программное обеспечение. Обеспечение безопасности операционных систем, приложений и служб. Обновление операционных систем и программного обеспечения. Тестирование уязвимостей.</p> <p>Тема 2.2. Безопасность хранения и передачи информации. Разрешения, шифрование данных, защита кабельной системы, защита беспровод-</p>

ных соединений, защита сетевого трафика. Защита периметра и интернет служб. Межсетевые экраны. Защита DNS, web, FTP серверов и сервера электронной почты. Защита удаленного управления и доступа к сети организации. Тема 2.3. Мониторинг безопасности. Удаленное управление (протоколы, службы). Удаленный доступ (типы, протоколы). Контрольные журналы. Обнаружение уязвимостей. Обнаружение вторжений. Следственный анализ.
---

#### 4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				

#### 4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	№ раздела дисциплины
Семестр 10			
1	Сканирование портов.	2	1
2	Получение информации об обновлениях.	2	1
3	Тестирование уязвимостей службы каталога	3	2
4	Тестирование уязвимости электронной переписки и обеспечение ее безопасности	3	2
5	Использование инструмента Nessus для обнаружения уязвимостей	2	2
Всего:		12	

#### 4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

#### 4.6. Самостоятельная работа студентов

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 10, час
Самостоятельная работа, всего	48	48
Изучение теоретического материала дисциплины	28	28
подготовка отчетов по лабораторным работам	12	12

Контрольные работы заочников	8	8
------------------------------	---	---

## 5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы студентов указаны в п.п. 8-10.

## 6. Перечень основной и дополнительной литературы

### 6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 Г96	Вычислительные системы, сети и телекоммуникации: учебник/А.И. Гусева, В.С. Киреев.- М.: Академия, 2014,- 288с.	40
004.4 Т18	Современные операционные системы=Modern operating system/Э. Таненбаум - 3-е издание -СПб.:Питер, 2015.-1120с.	40

### 6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
	Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. [Электронный ресурс] М. -ДМК Пресс, 2012, 592 с. - Режим доступа: <a href="http://e.lanbook.com/view/book/3032">http://e.lanbook.com/view/book/3032</a>	
	Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: <a href="http://znanium.com/bookread2.php?book=503511">http://znanium.com/bookread2.php?book=503511</a>	
	Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с/ - Режим доступа: <a href="http://znanium.com/bookread2.php?book=489084">http://znanium.com/bookread2.php?book=489084</a>	

## 7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование
	Не предусмотрено

## 8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

### 8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
1	Oracle Linux (Открытая операционная система на базе GNU/Linux)

### 8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Открытая система дистанционного обучения MOODLE

## 9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Лаборатория Открытых Информационных технологий	М. а. 22-10
3	Система дистанционного обучения	М. а. 22-10

## 10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Зачет	Список вопросов

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОПК-5	«способность решать стандартные задачи профессиональной деятельности на основе



информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности»	
1	Информатика
1	Введение в направление
3	Нормативная документация
7	Защита информации
10	Теория вычислительных процессов
10	Технологии информационной безопасности вычислительных систем
10	Введение в ортогональные преобразования информации
10	Производственная преддипломная практика

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4–балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
$85 \leq K \leq 100$	«отлично» «зачтено»	<ul style="list-style-type: none"> <li>- обучающийся глубоко и всесторонне усвоил программный материал;</li> <li>- уверенно, логично, последовательно и грамотно его излагает;</li> <li>- опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления;</li> <li>- умело обосновывает и аргументирует выдвигаемые им идеи;</li> <li>- делает выводы и обобщения;</li> <li>- свободно владеет системой специализированных понятий.</li> </ul>
$70 \leq K \leq 84$	«хорошо» «зачтено»	<ul style="list-style-type: none"> <li>- обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;</li> <li>- не допускает существенных неточностей;</li> <li>- увязывает усвоенные знания с практической деятельностью направления;</li> <li>- аргументирует научные положения;</li> <li>- делает выводы и обобщения;</li> <li>- владеет системой специализированных понятий.</li> </ul>
$55 \leq K \leq 69$	«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> <li>- обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;</li> <li>- допускает несущественные ошибки и неточности;</li> <li>- испытывает затруднения в практическом применении знаний направления;</li> <li>- слабо аргументирует научные положения;</li> <li>- затрудняется в формулировании выводов и обобщений;</li> <li>- частично владеет системой специализированных понятий.</li> </ul>
$K \leq 54$	«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> <li>- обучающийся не усвоил значительной части программного материала;</li> <li>- допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>- испытывает трудности в практическом применении знаний;</li> </ul>

		- не может аргументировать научные положения; - не формулирует выводов и обобщений.
--	--	--

#### 10.4. Типовые контрольные задания или иные материалы:

##### 1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	Учебным планом не предусмотрено

##### 2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
1	Сетевая инфраструктура организации и ее компоненты.
2	Анализ рисков и оборонительные модели.
3	Роли и ответственности.
4	Управление жизненным циклом безопасности.
5	Службы мониторинга безопасности.
6	Уровни защиты информационных систем.
7	Системы защиты элементов сетевой инфраструктуры.
8	Криптография в обеспечении информационной безопасности.
9	Алгоритмы шифрования.
10	Обнаружение нарушения целостности.
11	Цикл жизни цифрового сертификата.
12	Атаки на сеть и программное обеспечение.
13	Обеспечение безопасности операционных систем, приложений и служб.
14	Тестирование уязвимостей.
15	Защита кабельной системы, беспроводных соединений, сетевого трафика.
16	Защита периметра и интернет служб.
17	Межсетевые экраны.
18	Защита DNS, web, FTP серверов и сервера электронной почты.
19	Защита удаленного управления и доступа к сети организации.
20	Удаленное управление (протоколы, службы).
21	Удаленный доступ (типы, протоколы).
22	Контрольные журналы.
23	Обнаружение уязвимостей.
24	Обнаружение вторжений.

##### 3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	Учебным планом не предусмотрено

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

## **11. Методические указания для обучающихся по освоению дисциплины**

Целью дисциплины является – получение студентами необходимых знаний, умений и навыков в области проектирования, и эксплуатации безопасных вычислительных систем и корпоративных сетей различного назначения.

### **Методические указания для обучающихся по освоению лекционного материала**

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

#### Планируемые результаты при освоении обучающимся лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходиться к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

#### Структура предоставления лекционного материала:

- Изложение теоретических вопросов, связанных с рассматриваемой темой
- Описание методов и алгоритмов, применяемых для обеспечения информационной безопасности вычислительных систем и сетей

- Демонстрация примеров решения задачи обеспечения информационной безопасности вычислительных систем и сетей
- Обобщение изложенного материала
- Ответы на возникающие вопросы по теме лекции.

### **Методические указания для обучающихся по прохождению лабораторных работ**

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с аппаратно-программным обеспечением.

### **Задание и требования к проведению лабораторных работ**

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению. В соответствии с заданием обучающийся должен подготовить необходимые данные, получить от преподавателя допуск к выполнению лабораторной работы, выполнить указанную последовательность действий, получить требуемые результаты, оформить и защитить отчет по лабораторной работе.

### **Структура и форма отчета о лабораторной работе**

Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы.

### **Требования к оформлению отчета о лабораторной работе**

По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП ([www.guar.ru](http://www.guar.ru)) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП ([www.guar.ru](http://www.guar.ru)) в разделе «Сектор нормативной документации».

### **Методические указания для обучающихся по прохождению самостоятельной работы**

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы, у обучающегося формируется целеобразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются учебно-методические материалы по дисциплине.

Для обучающихся по заочной форме обучения читаются установочные лекции. Полный лекционный курс они изучают самостоятельно.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

### **Методические указания для обучающихся по прохождению промежуточной аттестации**

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

- зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

## Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой