



Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



«УТВЕРЖДАЮ»

Проректор по учебно-методической работе

Н.В. Бабина

«28» апреля 2020 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«ИСТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ В РФ»

Направление подготовки: 10.03.01 Информационная безопасность

**Профиль: Информационно-аналитические системы
финансового мониторинга**

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

Автор: к.в.н., доцент Воронов А.Н. Рабочая программа дисциплины: «История защиты информации в РФ». – Королев МО: «Технологический университет», 2020.

Рецензент: к.в.н., доцент Соляной В.Н.

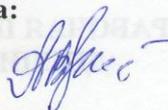
Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н. к.в.н. доцент			
Год утверждения (переподтверждения)	2020	2021	2022	2023
Номер и дата протокола заседания кафедры	Протокол № 8 от 26.03.2020			

Рабочая программа согласована:

Руководитель ОПОП ВО



к.в.н., доцент Воронов А.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переподтверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

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

Целью изучения дисциплины является формирование у студентов специализированной базы знаний по истории и тенденциям развития системы защиты информации в России с XV по XXI век, а также её современной организации и получение первичных навыков в формировании исторического опыта и перспектив развития подобных систем.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

Общепрофессиональные компетенции:

- (ОПК-4) способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

Профессиональные компетенции:

- (ПК-9) способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

Основными задачами дисциплины являются:

- ознакомление студентов с процессами становления и развития системы защиты информации в России, с государственной политикой и деятельностью органов защиты информации в различные периоды развития государства, с процессами развития и совершенствования нормативной базы по защите информации;
- формирование у студентов способности самостоятельно анализировать и использовать исторический опыт, основные тенденции, принципы, методы и компоненты системы защиты информации в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам в России.

После завершения освоения данной дисциплины студент должен:

Знать:

- основные предпосылки формирования системы защиты информации в России в XV – XVII веках;
- организацию и совершенствование системы защиты информации в Российской империи в XVIII-XIX веке;

- особенности системы защиты информации в начале XX века;
- организацию защиты информации в период промышленного подъёма (1900-1913 г.г.) и в период Первой мировой войны;
- основные особенности организации защиты информации в советский период, в годы гражданской войны, в период НЭПа и в 30-е годы становления советского государства;
- особенности защиты государственных секретов накануне и в период Великой Отечественной войны;
- направления и особенности совершенствования системы защиты информации в послевоенный период;
- основные особенности организации защиты информации на современном этапе развития России;
- современное состояние системы защиты информации в России и перспективы её совершенствования;

Уметь:

- классифицировать объекты и средства защиты информации в России в различные исторические периоды;
- правильно проводить анализ угроз информационной безопасности в стране и определять факторы, влияющие на требуемый уровень защиты информации;
- проводить анализ защищённости объектов на основе исторического опыта и определять классы защиты информации;
- анализировать факторы, определяющие организацию современной системы защиты информации в России и тенденции её развития;
- использовать положительные исторические уроки применения элементов системы защиты информации в России в различные исторические периоды развития нашей страны;
- правильно определять ближайшие перспективы развития системы защиты информации в России и тенденции её развития;

Владеть навыками:

- применения основных методов обработки и анализа исторических данных и опыта по защите информации;
- выявления и анализа потенциально существующих угроз безопасности государственным объектам и информации на основе исторического опыта; отнесения информации к государственной и другим видам тайны.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «История защиты информации в РФ» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01

«Информационная безопасность», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «История», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности» и компетенциях: ОК-3,4,5, ОПК-4,5 и ПК-8,10,15.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационно-психологическая безопасность персонала предприятия», «Защита общества от информации, запрещенной к распространению», «Финансовые институты», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетные единицы, 108 часов.

Таблица 1

Виды занятий	Всего часов	Семестр 5	Се- местр 6	Се- местр	Се- местр
Общая трудоемкость	108	108	-	-	-
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	60	60			
Курсовые, расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)	Тест 1,2	Тест 1,2			
Вид итогового контроля	Зачёт с оценкой	Зачёт с оценкой			

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час. Очное	Занятия в ин- терактивной форме, час. Очное	Код компетенций
Тема 1. Исторические аспекты формирования системы защиты информации в древние времена и в средневековье.	1	2	1	ОПК-4
Тема 2. Организация защиты информации в Российской империи в XVII - XIX веке.	2	2	1	ОПК-4
Тема 3. Особенности системы защиты информации в начале XX века.	2	4	1	ОПК-4
Тема 4. Становление системы защиты информации в Советском государстве после революции.	2	4	1	ОПК-4
Тема 5. Укрепление системы защиты государственных секретов в период Великой Отечественной войны.	2	4	1	ОПК-4
Тема 6. Организация защиты информации в послевоенный период.	2	4	1	ОПК-4, ПК-9
Тема 7. Основные особенности организации защиты информации на современном этапе.	2	4	1	ОПК-4, ПК-9
Тема 8. Современное состояние системы защиты информации и перспективы её совершенствования.	2	4	1	ОПК-4, ПК-9
Тема 9. Операции информационного противоборства в контексте международного права.	1	4	1/	ОПК-4, ПК-9
Итого:	16	32	9	

4.2. Содержание тем дисциплины

Тема 1. Исторические аспекты формирования системы защиты информации в древние времена и в средневековье.

Характеристика исторических этапов информационного противоборства стран и народов и их особенности. Формирование процессов защиты информации в древние времена. Опыт информационного противоборства древнеегипетских, ассирийских правителей, полководцев Рима и Греции, древних философов Китая и Европы. Роль религии и народного творчества в воспитании и поддержании русских традиций в княжеской и царской России. Система обеспечения безопасности и «опричнина». Основные функции в области внешней и внутренней политики государства и защиты информации. Методы защиты информации от иностранных государств, ограничения на въезд в Россию, дезинформация, ограничения на контакты и продвижения послов. Ответственность за шпионаж и государственную измену.

Тема 2. Организация защиты информации в Российской империи в XVII - XIX веке.

Особенности информационного противоборства в России в петровские и екатерининские времена. Органы защиты информации. Функции в области защиты информации Преображенского приказа и Верховного тайного совета. Деятельность военной коллегии и коллегии иностранных дел в области защиты информации. Основные функции тайной розыскных дел канцелярии и тайной экспедиции. Основные направления и методы защиты информации. Совершенствование шифрованной переписки. Ответственность за разглашение защищаемых сведений. Органы защиты информации. Основные задачи и деятельность отделений собственной его императорского величества канцелярии и секретного комитета.

Тема 3. Особенности системы защиты информации в начале XX века.

Информационное противоборство в период начала XX века перед первой мировой войной. Органы защиты информации. Функции Государственной думы, Государственного Совета, Комитета министров в области защиты информации. Деятельность "Особого совещания" в области координации важнейших вопросов внутренней политики и государственной безопасности. Функции в области защиты государственной тайны Главного управления Генерального штаба. Регламентация вопросов подбора и сохранения сети секретной агентуры. Организация секретного делопроизводства и шифрованной переписки. Особенности защиты информации в ходе первой мировой войны. Возрастание угроз защищаемой информации, основные направления и методы её защиты. Введение повсеместной предварительной цензуры для печати. Ответственность за разглашение защищаемых сведений.

Тема 4. Становление системы защиты информации в Советском государстве после революции.

Информационное противоборство Советского государства с иностранными спецслужбами и эмигрантскими организациями в 20-30 годы. Изменение политического и экономического строя страны, его влияние на организацию защиты информации. Резкое увеличение объёма сведений, составляющих государственную тайну. Объективные и субъективные причины расширения состава защищаемой информации. Возрастание угроз защищаемой информации и появления новых каналов несанкционированного доступа к ней. Активизация деятельности спецслужб иностранных государств по добыванию защищаемой информации о политическом, экономическом и военном положении СССР. Усиление роли государства в области защиты информации. Централизация управления защитой государственных секретов. Создание специальных органов защиты информации. Повышение ответственности за разглашение государственной тайны. Международные и внутриполитические факторы, оказавшие влияние на политику государства в области защиты информации. Направления и методы деятельности антисоветских организаций и иностранных разведок по добыванию секретной военной информации. Основные задачи органов военной контрразведки.

Тема 5. Укрепление системы защиты государственных секретов в период Великой Отечественной войны.

Информационное противоборство в начальный период Великой Отечественной войны. Активизация разведывательной деятельности фашистской Германии. Реорганизация разведывательных служб. Направления и методы добывания информации о военно-экономическом потенциале СССР. Государственная политика в области защиты военных, экономических и политических секретов. Регламентация вопросов защиты информации в нормативных документах. Расширение объектов защиты. Государственные и ведомственные органы защиты информации. Укрепление тыла, усиление охраны предприятий. Повышение персональной ответственности руководителей за организацию защиты государственных секретов. Усиление ответственности за разглашение государственной тайны и утрату документов, содержащих государственную тайну. Направления и методы деятельности государственных органов военной разведки и контрразведки по добыванию секретной военной информации. Исторические этапы противоборства в области криптоанализа и шифрования информации в ходе Второй мировой войны.

Тема 6. Организация защиты информации в послевоенный период.

Усиление разведывательных органов капиталистических стран. Появление дополнительных методов и средств несанкционированного получения информации. Государственная политика в области защиты информации. Ужесточение требований по обеспечению режима секретности. Меры по усилению охраны режимных предприятий. Повышение значимости норма-

тивных документов по вопросам защиты информации. Органы защиты государственных секретов. Появление новых видов носителей информации, средств и способов её обработки, хранения и передачи. Расширение угроз защищаемой информации и каналов несанкционированного доступа к ней. Объекты защиты. Появление новых направлений защиты информации, совершенствование методов защиты, разработка программно-аппаратных средств защиты. Информационное противоборство разведывательных и контрразведывательных органов двух противостоящих блоков государств.

Тема 7. Основные особенности организации защиты информации на современном этапе.

Информационное противоборство в системе политических отношений современного информационного общества. Факторы, оказывающие влияние на состав защищаемой информации и систему её защиты в политической, военной и экономической сферах деятельности государства. Возрождение коммерческой тайны. Расширение объектов защиты. Возрастание угроз защищаемой информации. Новые причины и условия проявления уязвимости информации. Совершенствование методов и средств несанкционированного получения информации. Государственная политика в области защиты информации. Децентрализация управления защитой информации. Реорганизация органов защиты информации в 90-е гг. Полномочия органов законодательной власти, Президента РФ, правительства и судебной власти в области защиты информации. Полномочия Совета безопасности и Межведомственной комиссии по защите государственной тайны.

Тема 8. Современное состояние системы защиты информации и перспективы её совершенствования.

Понятие информационной войны. Порядок применения средств и методов информационного воздействия на население нашей страны. Необходимость правильного выбора защитных информационных акций со стороны Российской Федерации, необходимость правильной расстановки сил и средств информационного противоборства в этих условиях. Особенности концепции национальной безопасности России. Уровень защищённости сведений, составляющих различные виды тайны. Вопросы, требующие государственного нормативного решения. Перспективы развития политики информационной безопасности нашего государства в ближайшем будущем.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для обучающихся по освоению дисциплины (модуля)» представлены в Приложении 2 настоящей программы.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведена в Приложении 1 к настоящей рабочей программе.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Анисимов А.А. Менеджмент в сфере информационной безопасности. Учебное пособие. – М.: Интернет – Университет информационных технологий / БИНОМ. Лаборатория знаний, 2010.
2. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность. Учебное пособие. – М.: «ФОРУМ», 2011.
3. Воронов А.Н. История и современная система защиты информации в России. Учебное пособие. – Королёв МО: КИУЭС, 2011.

Дополнительная литература:

1. Воронцова Л. В., Фролов Д. Б. История и современность информационного противоборства. М.: «Горячая линия – Телеком», 2006.
2. Волконский Н. Л. История информационных войн. Части I, II. – СПб.: ООО «Издательство – Полигон», 2003.
3. Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций. М.: «Гелиос АРВ», 2008.

Рекомендуемая литература:

1. Белов Е. Б., Лось В.П., Мещеряков Р.В., Шелупанов А. А. Основы информационной безопасности. Учебное пособие. М.: «Горячая линия – Телеком», 2006.
2. Вепринцев В. Б., Манойло А. В., Петренко А. И., Фролов Д. Б. Операции информационно - психологической войны. Краткий энциклопедический словарь-справочник. М.: «Горячая линия – Телеком», 2005.
3. Тихонов В. А., Райх В. В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. Учебное пособие. М.: «Гелиос АРВ», 2006.
4. Потапов В. В. Тайная история России. М.: «Мартин», 2008.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. <http://www.biblioclub.ru>
2. <http://znanium.com>
3. Энциклопедия информационной безопасности. – Публикации, статьи (www.wikIsec.ru).

Электронные образовательные ресурсы:

1. Учебный портал с электронно-методическими комплексами (do.kimes).
2. Универсальная библиотека онлайн (www.biblioclub.ru).
3. Polpred.com (www.polpred.com).
4. Единое окно доступа (www.window.edu.ru).
5. Издательский дом «Гребенников» (<http://grebennikov.ru/>).
6. ЭБС «Рукопт» (www.rucont.ru).
7. Электронные книги: электронная библиотека пособий на компакт дисках. ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348.

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

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

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы: Информационно – справочные (справочные) системы: «Гарант» (garant-center.ru), «Кодекс» (doskainfo.ru/advert/64804/), «Консультант +» (artiks.ru).

Ресурсы информационно-образовательной среды МГОТУ:

Рабочая программа и методическое обеспечение по курсу «История защиты информации в РФ».

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов

Практические занятия:

- Аудитория, снабжённая достаточным количеством посадочных мест, исходя из списочной численности группы
 - рабочее место преподавателя, оснащённое ПК;
 - рабочие места студентов, оснащенные компьютерами с доступом в глобальную сеть Интернет.
 - медиа-проектор с пультом управления и ПК;
 - для проведения практических занятий с применением активных и интерактивных технологий необходимо иметь компьютерные классы с оборудованными автоматизированными рабочими местами для студентов и преподавателя.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

***ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ**

**«ИСТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ В РФ»
(Приложение 1 к рабочей программе)**

Направление подготовки: 10.03.01 «Информационная безопасность»

**Профиль: Информационно-аналитические системы
финансового мониторинга**

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				знать	уметь	владеть
1	ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Тема 1 - 7	<ul style="list-style-type: none"> - основные предпосылки формирования системы защиты информации в России в XV – XVII веках; - организацию и совершенствование системы защиты информации в Российской империи в XVIII-XIX веке; - особенности системы защиты информации в начале XX века; - организацию защиты информации в период промышленного подъёма (1900-1913 г.г.) и в период Первой мировой войны; - основные особенности организации защиты информации в советский период, в годы гражданской войны, в период НЭПа и в 30-е годы становления со- 	<ul style="list-style-type: none"> - классифицировать объекты и средства защиты информации в России в различные исторические периоды; - правильно проводить анализ угроз информационной безопасности в стране и определять факторы, влияющие на требуемый уровень защиты информации; - проводить анализ защищённости объектов на основе исторического опыта и определять классы защиты информации; - анализировать факторы, определяющие организацию современной системы защиты информа- 	<ul style="list-style-type: none"> навыками - применения основных методов обработки и анализа исторических данных и опыта по защите информации; - выявления и анализа потенциально существующих угроз безопасности государственным объектам и информации на основе исторического опыта;

				ветского государства; - особенности защиты государственных секретов накануне и в период Великой Отечественной войны; - направления и особенности совершенствования системы защиты информации в послевоенный период;	ции в России и тенденции её развития;	
2	ПК-9	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Тема 8 - 9	- основные особенности организации защиты информации на современном этапе развития России; - современное состояние системы защиты информации в России и перспективы её совершенствования;	- использовать положительные исторические уроки применения элементов системы защиты информации в России в различные исторические периоды развития нашей страны; - правильно определять ближайшие перспективы развития системы защиты информации в России и тенденции её развития;	навыками - отнесения информации к государственной и другим видам тайны

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-4	Доклад (возможно групповая работа в составе 3 человек) в форме презентации и представления мини-исследования по тематике	А) полностью сформирована – 5 баллов Б) частично сформирована	Проводится устно с использованием мультимедийных систем, а также с использованием техни-

		<p>– 3-4 балла В) не сформирована- менее 2 и менее баллов</p>	<p>ческих средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов -5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.</p>
ПК-9	Контрольная работа	<p>А) полностью сформирована 5 баллов В) частично сформирована 3-4 балла С) не сформирована</p>	<p>1. Проводится в форме письменной работы 2.Время, отведенное на процедуру – 90 мин. Неявка – 0.</p>

		рована 2 балла	Критерии оценки: 1.Соответствие ответа уровню формирования компетенции (0-5 баллов). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
--	--	-------------------	--

3. 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

Примерная тематика докладов в презентационной форме:

1. Исторические предпосылки формирования системы защиты информации в России.
2. Особенности формирования и развития системы защиты информации в Российской империи.
3. Особенности формирования и развития системы защиты информации в советский период развития нашего государства.
4. Особенности формирования и развития системы защиты информации в России в постсоветский период.
5. Понятие «защита информации» как процесс, направленный на безопасность общества.
6. История становления и организация системы защиты информации в Российской империи в XVIII – XIX веке.
7. История становления и организация системы защиты информации в Российской империи в конце XIX, начале XX века.
8. Основные направления и методы защиты информации в Российской империи в XVII – XVIII веке.
9. Основные направления и методы защиты информации в Российской империи накануне и в ходе Первой мировой войны.
10. История появления и организация защиты государственной тайны в Российской империи.
11. История появления и организация защиты коммерческой тайны в Российской империи.

ской империи.

12. История появления и организация защиты банковской тайны в Российской империи.
13. История становления понятия «защита информации», информационная безопасность в системе наук Российской империи.
14. История организации разведывательно-аналитической деятельности служб безопасности в России.
15. Использование опыта по защите информации в Российской империи при организации защиты информации в СССР и в современных условиях.
16. Место и специфика истории защиты информации как направления в истории науки и техники Советского государства и постсоветской России.
17. Исторические предпосылки возникновения и развития локальных сетей и их защиты в нашей стране.
18. Основные исторические этапы становления защиты информации в сети Интернет в нашей стране и их особенности.
19. Стратегическая направленность и инструментальный базис защиты информации в России на современном этапе.
20. История возникновения и особенности развития организационных структур, выполняющих защиту информации в России.

Примерная тематика реферата:

1. Исторические предпосылки формирования информационного общества в России и особенности его информационной безопасности.
2. Особенности и исторические уроки развития системы защиты информации в СССР.
3. Человек и информационное общество в исторической ретроспективе и на современном этапе развития государства.
4. История развития технических систем промышленного шпионажа.
5. История развития закладных устройств - теория и процесс их использования.
6. Становление и развитие нормативной базы защиты информации в Российской империи в XVII – XVIII веке.
7. Становление и развитие нормативной базы защиты информации в Российской империи в XIX, начале XX века.
8. Основные этапы становления и развития стандартов в области информационной безопасности России.
9. Становление и развитие авторского права в Российской империи и на современном этапе развития нашей страны.
10. Становление и развитие патентного права в Российской империи и на современном этапе развития нашей страны.
11. Организация защиты информации в акционерных компаниях в Российской империи и на современном этапе развития нашей страны.
12. Защита информации в банковских учреждениях Российской империи и на современном этапе развития нашей страны.

13. Защита информации в процессе биржевой деятельности в России.
14. Защита информации в торговых компаниях Российской империи и на современном этапе развития нашей страны.
15. Организация защиты информации в Министерстве иностранных дел Российской империи и на современном этапе развития нашей страны.
16. Совершенствование системы защиты информации в России в конце XIX–начале XX века.
17. Совершенствование системы защиты информации в СССР в период Второй мировой войны.
18. Совершенствование системы защиты информации в СССР в период холодной войны с западными державами.
19. История появления и развития секретного делопроизводства в России.
20. Перспективы использования информационных технологий, направленных на защиту информации в России.

Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один или несколько вариантов ответа.

Вопросы

1-ое промежуточное тестирование (Т1)

1. Что понимают под информационным противоборством в современном мире?
 - это межгосударственное военное противодействие, осуществляемое путём программно-технического, радиоэлектронного и физического поражения инфраструктуры государства, дезорганизации его управления, дезориентации политического руководства, а также оказания психологического воздействия на население страны;
 - это процесс выделения деятельности по доведению информации до широких масс сначала в отдельную функцию трудовой деятельности, затем в род трудовой деятельности и наконец, в особую профессиональную деятельность человечества;
 - это совокупность взаимоотношений между субъектами мирового сообщества, в рамках которых данные субъекты путём воздействия на информационную сферу друг друга стремятся решить свои задачи в различных областях жизнедеятельности, а так же препятствуют аналогичной деятельности у других;
 - это способность государства и общества обеспечить с определённой вероятностью достаточные и защищённые информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности, а также устойчи-

вого функционирования и развития, способность противостоять информационным опасностям и угрозам, негативным информационным воздействиям на общественное сознание и психику людей.

2. Организация псевдосенсаций входила в набор методов манипулирования общественным мнением, которые придумал Платон?

- да;
- нет.

3. Выберите основные составляющие психики человека, которые выделил Аристотель в

качестве основных объектов информационного воздействия:

- ощущения;
- сознание;
- воля;
- чувства.

4. Что означают вербальные технологии информационного воздействия на массы

населения?

- воздействие на людей с помощью печатных средств доставки информации;
- воздействие на людей с помощью технических средств распространения информации;
- воздействие на психику человека с помощью устной речи и наглядных демонстрационных средств;
- воздействие на людей с помощью телекоммуникационных систем и средств.

5. Что необходимо было предпринять, по мнению древнекитайского философа Сунь Цзы, чтобы покорить противника без сражения:

- разрушить планы противника;
- расстроить союзы противника;
- распространить угрожающие слухи;
- разгромить войска противника;

6. Выберите основные силы, которые играли главную роль в воспитании населения России в древности:

- Религия;
- Народное творчество;
- Армия;
- Полиция.

7. Устрашение входило в основные методы информационного воздействия на население в древние времена?

- да;

- нет.

8. Агитация входила в основные формы доведения информации до широких масс населения в древние времена?

- да;
- нет.

9. Выберите основные органы, которые боролись с иноверцами при Иване Грозном:

- Тайная канцелярия;
- Преображенский приказ;
- Посольский приказ;
- Чёрные кабинеты.

10. Где и когда была организована первая государственная почтовая служба в Европе?

- в Австрии в XVII веке;
- в Германии в XV веке;
- в Англии в XIV веке;
- во Франции в XVI веке.

11. Кто и где впервые ввёл «Чёрные кабинеты» для проверки корреспонденции?

- Король Генрих IV во Франции;
- Король Леопольд I в Австрии;
- Королева Елизавета I в Англии;
- Император Пётр I в России.

12. Что такое перлюстрация?

- дешифрирование перехваченной корреспонденции с помощью методов криптоанализа;
- сокрытие самого факта секретной переписки между корреспондентами;
- тайное безуликовое вскрытие корреспонденции и копирование её содержания;
- шифрование передаваемого сообщения с помощью случайных кодовых комбинаций.

13. Кто был выдающимся дешифровальщиком XVI века во Франции?

- Франсуа Виет;
- Джордж Сквелл;
- Эжен Базери;
- Жак Фуше.

14. Кто впервые ввёл «Чёрные кабинеты» в России в 1742 году?

- Ордин-Нащёкин;

- Бестужев-Рюмин;
- Бенкендорф;
- Рылеев-Пестель.

15. Какой орган занимался организацией шифровальной службы в России при царе Алексее Михайловиче?

- Министерство иностранных дел;
- Тайная канцелярия;
- Приказ тайных дел;
- Преображенский приказ.

16. Выберите основные органы, которые боролись с вражеской дезинформацией и клеветой при Петре I:

- Преображенский приказ;
- Тайная канцелярия;
- Разведка и контрразведка;
- Министерство иностранных дел;
- Пограничная служба;
- Третье отделение его императорского величества.

17. Кто и когда впервые изобрёл книжный шифр?

- Эжен Базери в 1742 году;
- Даниель Дефо в 1654 году;
- Оливер Кромвель в 1786 году;
- Джордж Сквел в 1811 году.

18. Выберите основные шифры, которые применялись в Европе в XVII - XVIII веке для пересылки важных сообщений:

- Петтит;
- Коды Номенклатора;
- Шифр Джефферсона.
- Код Португальской армии.

19. Кто впервые выделил прессу в качестве объекта контрразведывательной деятельности?

- Джонатан Свифт;
- Антуан Россиньоль;
- Жак Фуше;
- Шарль Талейран.

20. Выберите основные методы достижения внешнеполитических целей, которые использовала Российская императрица Екатерина II:

- психологическая обработка союзников и противников;
- распространение псевдосенсаций среди широких масс населения;

- разложение противников изнутри путём использования их внутренних противоречий;
- распространение печатных средств за границей.

21. Выберите экспедиции, которые входили в Министерство иностранных дел, которое было создано в России по указу Александра I в начале XIX века:

- цифирная;
- антицифирная;
- газетная;
- перлюстрации.

22. Какой орган был создан в России для раскрытия заговоров после восстания декабристов на Сенатской площади в 1825 году?

- Тайная канцелярия;
- Третье отделение собственной его императорского величества канцелярии;
- Особый отдел генерального штаба Российской империи;
- Отделение юстиции его императорского величества.

23. Когда и где в России было создано первое телеграфное агентство?

- в Москве в 1901 году;
- в Санкт-Петербурге в 1904 году;
- в Ростове в 1905 году.
- во Владивостоке в 1907 году.

24. Выберите страны, входившие в Тройственный союз накануне Первой мировой войны:

- Германия;
- Австро-Венгрия;
- Англия;
- Италия.

25. Сидней Рейли относился к знаменитым российским разведчикам в начале XX века?

- да;
- нет.

26. Когда и по чьей инициативе в России впервые была создана официальная государственная структура контрразведки?

- в 1904 году по инициативе министра финансов Коковцева;
- в 1903 году по инициативе военного министра Куропаткина;
- в 1900 году по инициативе генерала Бенкендорфа;
- в 1901 году по инициативе министра иностранных дел Воронцова;

27. Известная французская танцовщица Мата Харри являлась российским агентом осведомителем в период Первой мировой войны?

- да;
- нет.

28. Принцип опережения пропагандистской деятельностью политических действий своего правительства являлся одним из важнейших принципов осуществления пропаганды по мнению лорда Нордкифа?

- да;
- нет.

29. В каком печатном источнике впервые в Европе после Первой мировой войны пропаганда была выделена как особый вид оружия?

- в книге К. Стюарта «Тайны дома Крю»;
- в книге Ф. Шенемана «Искусство влияния на массы людей»;
- в книге И. Пленге «Немецкая пропаганда»;
- в книге Гарольда Лассвеля «Техника пропаганды в мировой войне».

30. Выберите стратегические цели пропаганды, которые сложились в ходе Первой мировой войны:

- возбуждение специфических интересов в отдельных группах населения, борьба с распространением нежелательных идей;
- возбуждение у собственного населения, а также у населения стран союзников и нейтральных стран ненависти к неприятелю;
- поддержание дружественных отношений с союзниками;
- сохранение добрых отношений с нейтральными странами, получение их поддержки и деморализация противника.

31. Выберите основные формы управления пропагандой, которые сложились в ходе Первой мировой войны в разных странах:

- единый исполнительный комитет в США;
- общая национальная комиссия во Франции;
- орган, в котором каждый исполнитель ответственен за свою отрасль деятельности, в Великобритании;
- общее информирование прессы представителями соответствующих отраслей государственного управления в Германии;

32. Выберите основные приёмы воздействия на широкие массы людей, которые сложились в ходе Первой мировой войны:

- осведомление;
- компрометация;
- агитация;
- пропаганда.

33. Агитацию относили к стратегической области печати?

- да;
- нет.

34. Пропаганду относили к тактической области печати?

- да;
- нет.

35. В чём заключалась суть операции «Трест», проводимой советскими спецслужбами в 1925 году?

- операция по вербовке иностранных осведомителей;
- операция по раскрытию военного заговора в высших эшелонах власти;
- операция по добыванию ключей к шифрам дипломатической переписки посольств;
- операция по разоблачению белоэмигрантского сопротивления.

2-ое промежуточное тестирование (Т2)

1. Когда и где началось формирование первых подразделений радиоразведки в молодой большевистской республике?

- в декабре 1918 года в подразделениях пограничной службы;
- в январе 1919 года в Красной армии и на флотах;
- в декабре 1920 года в разведывательно-пеленгаторных службах армии;
- в январе 1921 года в спецотделах ВЧК;

2. Какой орган впервые был создан у нас в стране 5 мая 1921 года, как единый центр криптографической службы и кто его возглавил?

- контрразведывательный отдел, который возглавил А. Х. Артузов;
- служба политконтроля при ОГПУ, которую возглавлял П. В. Макаров;
- специальный отдел при ВЧК, который возглавил Глеб Бокий;
- отделение иностранного отдела при ОГПУ, которое возглавлял П. А.

Литвинов.

3. Надзор за магазинами и складами входил в задачи службы политконтроля при ОГПУ в СССР?

- да;
- нет;

4. Кто в советской разведке работал под псевдонимом «Ганс»?

- Н.А. Кузнецов;
- Д. А. Быстролётов;
- Вилли Леман;
- Рихард Зорге.

5. Вили Леман был завербованным сотрудником немецкой разведки «Абвер» в начале Второй мировой войны?

- да;
- нет;

6. Какой шифр применяли военно-морские силы США в 30-е годы XX века?

- шифр микроточек;
- полиалфавитный шифр;
- шифр полосы;
- пурпурный код.

7. Когда и где впервые было создано министерство пропаганды, кто его возглавил?

- в 1940 г. в Великобритании – Черчилль;
- в 1937 г. во Франции – Маршан;
- в 1935 г. в США – Ярдли;
- в 1933 г. в Германии - Гебельс.

8. Войска пропаганды впервые были созданы в США в 1938 году?

- да;
- нет;

9. Первые военно-журналистские игры накануне Второй мировой войны проводились?

- в СССР;
- в Великобритании;
- во Франции;
- в США;

10. Кто работал на советскую разведку под псевдонимом «Рамзай» и где это происходило в 30-е – 40-е годы XX века?

- Дмитрий Быстролётов в Италии;
- Рихард Зорге в Японии;
- Шандор Радо в Швейцарии;
- Гай Бёрджес в Великобритании;

11. Как называлась стратегическая дезинформационная операция фашистской Германии, направленная на скрытие основных мероприятий по подготовке к нападению на СССР в 1941 году?

- «Ледокол»
- «Ультра»;
- «Морской лев»;
- «Барбаросса».

12. Какую шифровальную машинку использовали немцы во Второй мировой войне для шифрования стратегических сообщений;

- шифратор Джефферсона;

- шифратор «М-209»;
- шифратор «Энигма»;
- шифратор вокодерных станций «X-ray».

13. Выберите правильные ключи для шифратора «Энигма»:

- коммутация дисков;
- выбор дисков из комплекта и взаимное расположение их в шифраторе;
- выбор и размещение шифровальной полосы;
- коммутации штепсельной панели.

14. В шифраторе «Энигма» присутствовал суточный ключ?

- да;
- нет;

15. Кто получил первые результаты по дешифрированию сообщений, зашифрованных «Энигмой»?

- французские криптоаналитики;
- английские криптографы, лингвисты и математики;
- дешифровальщики СССР;
- польские криптоаналитики.

16. Какая операция проводилась англичанами по дешифрированию «Энигмы» в усадьбе Блетчли-Парк графства Бэкингемшир?

- «Престол»;
- «Ультра»;
- «Люси»;
- «Хагелин».

17. В какой стране и под видом кого работал легендарный советский разведчик Рихард Зорге в конце 30-х начале 40-х годов XX века?

- под видом владельца фотоателье в Германии;
- под видом немецкого коммерсанта в Австрии;
- под видом немецкого журналиста в Японии;
- под видом сотрудника посольства в Италии.

18. В чём суть операции «Монастырь» и когда она проводилась?

- создание разведгруппы на территории Бельгии из сети «Красная капелла» в 1941 году;
- создание подпольной монархической организации «Престол» на территории СССР под контролем НКВД в 1942 году;
- организация работ по дешифрированию сообщений, закодированных с помощью шифратора «Энигма» в 1943 году;
- операция по добыванию ключей к японским шифрам в Шанхае в 1940 году.

19. Кто из советских разведчиков работал под псевдонимом «Гейне» при организации радиоигр в 1942 году?

- Н. Кузнецов;
- Шандор Радо;
- Ким Филби ;
- А. Демьянов.

20. Выберите основные приёмы для дезинформирования противника, которые использовали спецслужбы Германии во II Мировой войне:

- распространение слухов;
- создание видимости утечки информации в результате несчастного случая;
- имитация активного интереса к стратегически неважным объектам;
- проведение пропагандистских операций.

21. Выберите основные принципы дезинформирования противника, которые использовали спецслужбы Германии во II Мировой войне:

- точная координация действий правительственных субъектов, участвующих в подобных мероприятиях;
- обеспечение правдивости информации, а не достоверности сообщаемых сведений;
- соблюдение секретности этих операций;
- своевременность проводимых мероприятий.

22. Выберите государственные организации фашистской Германии, которые вели активную пропагандистскую деятельность против СССР в ходе Великой Отечественной войны:

- служба пропаганды в восточных районах «Винета»;
- институт геополитики;
- диверсионный отряд «Унтернемен-цепелин»;
- национально-трудовой союз нового поколения.

23. Организация «Нордическое общество» относится к негосударственным структурам фашистской Германии, которые вели активную пропагандистскую деятельность против СССР во II Мировой войне?

- да;
- нет;

24. Организация «Иберогерманский институт» относится к негосударственным структурам фашистской Германии, которые вели активную пропагандистскую деятельность против СССР во II Мировой войне?

- да;
- нет;

25. Выберите основные способы, которыми действовала Советская контрразведка для дезинформирования противника во 2-м и 3-м периодах Великой Отечественной войны?

- пропаганда среди военнопленных;
- ведение радиоигр;
- осуществление дезинформации через завербованных агентов;
- проведение пропагандистских операций.

26. Когда и где был впервые создан Совет военно-политической пропаганды в СССР?

- в 1941 году при Совинформбюро СССР;
- в 1942 году при Главном политическом управлении СССР;
- в 1943 году при Совнаркоме СССР;
- в 1945 году при Министерстве иностранных дел СССР.

27. Что было создано под руководством знаменитого математика Алана Тьюринга в конце 1942 года в Англии?

- шифратор вокодерных станций «SIGSALY»;
- электромеханическая вычислительная машина «Паук»;
- первая электромеханическая вычислительная машина «Бомба»;
- шифратор «M-209».

28. Сколько всего было проведено пропагандистских операций Советским командованием в 1944 – 1945 годах в ходе Великой Отечественной войны?

- 27;
- 10;
- 5;
- 2.

29. Что понимается в мире под военным конфликтом?

- это межгосударственное военное противоборство, осуществляемое путём программно-технического, радиоэлектронного и физического поражения инфраструктуры государства, дезорганизации его управления, дезориентации политического руководства, а также оказания информационно-психологического воздействия на население страны;

- это столкновение интересов различных социальных групп или социально-политических субъектов, а так же противоборство форм разрешения противоречий между ними с применением политических, экономических и военных средств борьбы или с применением силы;

- это совокупность средств, методов и способов для нанесения ущерба информационной сфере противника, а также процессам, функционирующим на основе информации;

- это совокупность организационных мероприятий и действий служб безопасности с применением технических средств, направленных на обеспечение установленного порядка и правил поведения персонала, а также предот-

вращение, обнаружение и ликвидацию угроз жизни людей, сохранение имущества и информации.

30. Как называлась операция по вводу советских войск в Венгрию и проведения пропагандистских действий при подавлении восстания в Венгрии в 1956 году?

- «Зефир»;
- «Люси»;
- «Анадырь»;
- «Вихрь».

31. Когда произошёл знаменитый Карибский кризис, когда человечество стояло на пороге III Мировой войны с применением оружия массового уничтожения?

- 1950 – 1953 год;
- 1953 – 1958 год;
- 1962 – 1964 год;
- 1965 – 1968 год.

32. Кто вводил свои войска в Чехословакию в августе 1968 года для подавления народного восстания в этой стране?

- только СССР;
- страны Варшавского Договора;
- страны НАТО;
- Пентагон США.

33. Выберите агентов, которые работали на разведку СССР в организации Кембриджская пятёрка:

- Рудольф Абель;
- Ким Филби;
- Джон Кернкросс;
- Энтони Блант.

34. Кто работал на советскую разведку в США под псевдонимом Марк в 50-х годах XX столетия?

- Дональд Маклейн;
- Гай Бёрджес;
- Вильям Фишер;
- Фрэнсис Пауэрс.

35. Выберите основные скрытые приёмы по передаче добытой информации, которые использовал советский резидент Рудольф Абель в 50-х годах XX столетия:

- микроточки с 35 мм. фотоплёнки;

- использование химических чернил для скрытия текста в обычных журналах;
- микротекст, который вкладывался в полое отверстие монеты;
- скрытие сообщения в полем конце карандаша.

36. Какой орган для проведения спецпропаганды действовал в составе советского ограниченного контингента войск в Афганистане на протяжении 1979 – 1989 года?

- временный информационный центр;
- отделение для ведения психологической войны;
- служба политконтроля;
- специальный агитотряд.

37. Какой орган был создан распоряжением Правительства РФ для информационного обеспечения операций федеральных сил за десять дней до того как федеральные войска вошли на территорию Чечни?

- бюро оперативной информации;
- министерство информации;
- временный информационный центр;
- пресс-служба при Роскомпечати РФ.

38. Выберите основные недостатки информационно-психологического обеспечения боевых действий в Чечне со стороны средств массовой информации РФ:

- бессистемность и непрофессионализм федеральных пресс-служб;
- не был определён порядок поступления информации в прессу и для общественности;
- конфликт с Министерством обороны РФ;
- система взглядов на информационное противодействие сильно устарела.

39. Где был организован Чеченский информационный центр для проведения антироссийской пропаганды сепаратистами в 1995 году?

- в Грозном;
- в Кракове;
- во Владикавказе;
- в Стамбуле.

40. Где размещался филиал радиостанции «Свободный Кавказ» для ведения антироссийского вещания на территорию России и стран Центральной Европы?

- в Москве;
- в Грозном;
- в Ростове на Дону;
- в Каунасе.

41. Какие специальные подразделения были сформированы в составе Российских вооружённых сил во второй Чеченской кампании в 1999 году для проведения пропагандистской деятельности?

- специальные агитотряды;
- отделения для ведения психологической войны;
- отделения для работы с гражданским персоналом;
- пресс-службы МО РФ;

42. Выберите самые распространённые методы фильтрации информации, которые используются в обществе западной демократии для создания заданного стереотипа общественного сознания и управления им:

- двухсторонний дезодоратор;
- открытый вентиль;
- временной селектор;
- информационная заслонка.

43. Информационное доминирование это базовый принцип информационного воздействия и одна из характеристик информационного оружия?

- да;
- нет;

44. Информационная асимметрия это наступательный принцип, заложенный в цель психологических операций?

- да;
- нет;

45. Концепция «Информационного сдерживания» разработана в США?

- да;
- нет;

46. Выберите основные подходы к определению информационной войны, которые вкладывают в это понятие современные учёные:

- как совокупность отдельных мероприятий и операций;
- как сфера военного противоборства;
- как область информационных взаимоотношений;
- как явление мирного периода государственных отношений.

47. Выберите виды информационного оружия, которые выделяют в зависимости от способа поражения:

- средства воздействия на психику людей;
- средства радиоэлектронной борьбы;
- средства программно-технического воздействия;
- средства контроля и управления доступом.

48. Трудность создания и сохранения коалиций входит в 7 характерных черт современной стратегической информационной войны?

- да;
- нет;

49. Отсутствие возможности предугадать направление и инструментарий возможной атаки входит в 7 основных различий между войной традиционной и информационной войной в современном мире?

- да;
- нет;

50. Выберите правильные виды информационно-психологических операций по характеру воздействия на сознание людей в обществе:

- пропагандистские;
- консолидирующие;
- манипулятивные;
- дезинформационные.

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

Формой контроля знаний по дисциплине «История защиты информации в РФ» являются две текущие аттестации в виде тестов и одна промежуточная аттестация в виде зачёта с оценкой в устной форме.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	1-е тестирование	ОПК-4	20 вопросов	Компьютерное тестирование; время ответное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.

					дуры	
Со-глас-но учеб-ному плану	2-е те-сти-ро-вание	ОПК-4, ПК-9	20 во-просов	Компьютерное тестирование; время отве-денное на про-цедуру – 30 ми-нут	Резуль-таты те-стиро-вания предо-ставля-ются в день про-веде-ния про-це-дуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 бал-лов.
Со-глас-но учеб-ному плану	Зачёт с оцен кой	ОПК-4, ПК-9	3 во-проса	Зачет с оценкой прово-дится в устной форме, путем ответа на во-просы. Время отве-денное на про-цедуру – 30 ми-нут.	Резуль-таты предо-ставля-ются в день про-веде-ния зачета с оценкой	Критерии оценки: Оценки «отлично» заслуживает ответ, содержащий: глубокое и систематиче-ское знание всего программного материала и структуры конкрет-ной дисциплины, а также ос-новного содержания и новаций лекционного курса по сравне-нию с учебной литературой; отчетливое и свободное владение концептуально-понятийным аппаратом, науч-ным языком и терминологией соответствующей научной обла-сти; знание основной литера-туры и знакомство с дополни-тельно рекомендованной лите-ратурой; умение выполнять предусмотренные программой задания; логически корректное и убедительное изложение ответа. Оценки «хорошо» заслуживает ответ, содержащий: знание узловых проблем программы и основного содер-

						<p>жания лекционного курса; умение пользоваться концептуально-понятийным аппаратом в процессе анализа основных проблем программы; знание важнейших работ из списка рекомендованной литературы; умение выполнять предусмотренные программой задания; в целом логически корректное, но не всегда точное и аргументированное изложение ответа. Оценки «удовлетворительно» заслуживает ответ, содержащий: фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ. Оценка «неудовлетворительно» ставится при: незнании либо отрывочном представлении учебно-программного материала; неумении выполнять предусмотренные программой задания.</p>
--	--	--	--	--	--	---

Типовые вопросы, выносимые на зачёт с оценкой:

1. Основные этапы развития информационной безопасности и их характеристика.
2. Аспекты информационной безопасности в различных сферах жизнедеятельности общества и государства.
3. Исторические этапы информационного противоборства стран и народов, их

- особенности и характеристика.
4. Что явилось важнейшим фактором, способствовавшим развитию информационного противоборства в мире?
 5. Формирование процессов защиты информации в древние времена.
 6. Какие методы манипуляции общественным мнением предложил Платон и в чём их актуальность?
 7. Какие органы боролись с иноверцами при Иване Грозном (IV), их состав и основные задачи?
 8. Характеристика информационного противоборства в средневековье и его особенности.
 9. Кто, когда и где впервые основал государственную почтовую службу в Европе, основные задачи и особенности её деятельности?
 10. Выдающиеся дешифровальщики XVI века и их основные заслуги по защите информации.
 11. Особенности информационного противоборства в России в Петровские времена.
 12. Какой орган занимался организацией шифровальной службы в России при царе Алексее Михайловиче, когда он был создан?
 13. Когда в России появились первые почтовые отделения и кто внёс основной вклад в становление и развитие этой службы?
 14. Развитие процессов защиты информации в России в Екатерининские времена.
 15. Где и когда впервые появились «Чёрные кабинеты», чем они занимались, кто и когда ввёл «Чёрные кабинеты» в России?
 16. Особенности информационного противоборства в России в XVIII – XIX веке.
 17. Кто, когда и где впервые изобрёл книжный шифр, какие ещё шифры применяли в тот период?
 18. Кто впервые выделил прессу в качестве субъекта и объекта контрразведывательной деятельности, что ещё было сделано в организационном плане для контрразведки в этот период истории?
 19. Когда и по чьему указу в России было учреждено министерство иностранных дел, кто его возглавил и какие экспедиции в него входили?
 20. Какой орган был создан в России после восстания декабристов в 1825 г. на Сенатской площади взамен тайной канцелярии и кто его возглавил?
 21. Информационное противоборство в период начала XX века перед Первой мировой войной.
 22. Особенности информационного противоборства в ходе Первой мировой войны.
 23. Уроки Первой мировой войны, достоинства и недостатки системы защиты информации Российской империи.
 24. Опыт пропаганды, агитации и защиты информации во внутривнутриполитической жизни России в период революции 1917 года.
 25. Опыт противоборства Советского государства с иностранными спецслужбами и эмигрантскими организациями в годы Гражданской войны и в 20-30

годы XX столетия.

26. Когда и где началось формирование первых подразделений радиоразведки в нашей стране?
27. Когда и какой орган впервые был создан у нас в стране как единый центр криптографической службы, кто был его начальником, основные особенности его работы?
28. Когда и где в СССР был создан первый контрразведывательный отдел, кто его возглавлял, его основные задачи и функции?
29. Когда и где у нас в стране появились первые разведывательно-пеленгаторные группы, какова была их численность и основные методы работы?
30. В чём заключалась суть операции «Трест», проводимой советскими спецслужбами в 1925 году?
31. В чём разница информирования, агитации и пропаганды с точки зрения воздействия на массы людей?
32. Кто и когда в Советской разведке работал под псевдонимом «Ганс», каковы его основные заслуги перед нашей страной, основные методы работы?
33. Информационное противоборство и роль средств массовой информации в СССР перед Второй мировой войной.
34. Что представлял собой шифратор Джефферсона, какой шифр в нём использовался, где и когда он применялся?
35. Уроки советской военной пропаганды накануне Великой Отечественной войны.
36. Кто такой Вилли Леман, в чём выражались его заслуги для нашей страны, основные особенности его работы и когда это было?
37. Что означает «Энигма», кто и когда её изобрёл, из чего она состоит, какие ключи использовались, порядок работы с ней?
38. Укрепление системы защиты государственных секретов в начальный период Великой Отечественной войны.
39. Кто из советских разведчиков работал под псевдонимом «Рамзай», где и когда это было, основные методы его работы?
40. Что означает операция «Ультра», где и когда она проводилась, почему так называлась и суть её проведения?
41. Пропагандистская деятельность стран – союзников СССР в ходе Второй мировой войны.
42. Какие основные приёмы для дезинформирования противника использовали спецслужбы Германии во Второй мировой войне?
43. Развитие советской пропаганды и защиты информации в годы Великой Отечественной войны.
44. В чём суть операции «Престол», когда она проводилась, с какой целью и кто был двойным агентом в ней?
45. Назовите основные принципы дезинформирования противника, используемые спецслужбами Германии во Второй мировой войне.
46. Когда впервые стали применяться пропагандистские операции наших войск, что они включали, сколько всего их было проведено и с какой целью?
47. Что было создано под руководством знаменитого математика Алана Тью-

- ринга в Англии в конце 1942 года и для чего использовалось?
48. Организация защиты информации в послевоенный период Советского государства.
 49. Роль информационного противоборства в локальных войнах и вооружённых конфликтах 50-70 годов XX столетия.
 50. Кембриджская пятёрка, состав и основные методы её работы.
 51. Какие приёмы для передачи сведений использовал наш резидент в США Рудольф Абель в 50-х годах XX века?
 52. Пропагандистское обеспечение военной акции СССР в Афганистане в 1979-89 году.
 53. Место и роль средств массовой информации в военных конфликтах 90-х годов XX столетия.
 54. Уроки информационного противоборства в Чеченском военном конфликте и его особенности.
 55. Информационное противоборство в системе политических отношений современного информационного общества.
 56. Информационное оружие как основное средство ведения информационных войн XXI века и его характеристика.
 57. Каковы основные различия между войной традиционной и информационной?
 58. Информационная асимметрия и информационное доминирование в современном мире, основные особенности информационного противоборства в XXI веке.
 59. Основные понятия концепции информационного сдерживания в современном мире.
 60. Современное состояние информационной безопасности России и перспективы её совершенствования.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ
ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ
ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

«ИСТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ В РФ»

(Приложение 2 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы

финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

1. Общие положения

Целью изучения дисциплины является формирование у студентов специализированной базы знаний по истории и тенденциям развития системы защиты информации в России с XV по XXI век, а также её современной организации и получение первичных навыков в формировании исторического опыта и перспектив развития подобных систем.

Основными **задачами** дисциплины являются:

- ознакомление студентов с процессами становления и развития системы защиты информации в России, с государственной политикой и деятельностью органов защиты информации в различные периоды развития государства, с процессами развития и совершенствования нормативной базы по защите информации;

- развитие навыков критического восприятия и оценки источников информации, умения аргументированно отстаивать собственное видение проблем и способов их разрешения, выработка навыков работы с оригинальными и адаптированными историческими текстами;

- формирование у студентов способности самостоятельно анализировать и использовать исторический опыт, основные тенденции, принципы, методы и компоненты системы защиты информации в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам в России.

2. Указания по проведению практических (семинарских) занятий

Практическое занятие 1.

Вид практического занятия: смешанная форма практического занятия.

Тема 1. Исторические аспекты формирования системы защиты информации в древние времена и в средневековье.

Содержание практического занятия:

Учебные вопросы:

1. Особенности вербального периода информационного противоборства в древние времена.
2. Функции Боярской думы в области внешней и внутренней политики и обеспечении безопасности государства.
3. Царский «тайный совет» и его роль в защите информации. Учреждение Приказа тайных дел и его функции.
4. Вопросы защиты информации в Судебниках XVI века.

Продолжительность занятия – 2 ч.

Практическое занятие 2.

Вид практического занятия: смешанная форма практического занятия.

Тема 2. Организация защиты информации в Российской империи в XVII - XIX веке.

Содержание практического занятия:

Учебные вопросы:

1. Особенности информационного противоборства в России в XVII – XVIII веке.
2. Совершенствование организации защиты информации в первой половине XIX века.
3. Формирование системы защиты информации во второй половине XIX века.

Продолжительность занятия – 2 ч.

Практическое занятие 3.

Вид практического занятия: смешанная форма практического занятия.

Тема 3. Особенности системы защиты информации в начале XX века.

Содержание практического занятия:

Учебные вопросы:

1. Организация защиты информации в период промышленного подъёма (1909 – 1913 годы).
2. Организация защиты информации в период Первой мировой войны.
3. Достоинства и недостатки системы защиты информации в Российской империи.

Продолжительность занятия – 4 ч.

Практическое занятие 4.

Вид практического занятия: доклад в форме презентации

Тема 4. Становление системы защиты информации в Советском государстве после революции.

Содержание практического занятия:

Учебные вопросы:

1. Организация защиты военной тайны в годы Гражданской войны.
2. Становление системы защиты государственных секретов в 20-е годы XX века.
3. Развитие системы защиты государственных секретов в 30-е годы XX века.

Продолжительность занятия – 4 ч.

Практическое занятие 5.

Вид практического занятия: доклад в форме презентации

Тема 5. Укрепление системы защиты государственных секретов в период Великой Отечественной войны.

Содержание практического занятия:

Учебные вопросы:

1. Основные направления и методы защиты государственных секретов в предвоенное время и в период действия военного положения.
2. Факторы, обусловившие состав защищаемой информации и организацию её защиты.
3. Пропагандистская деятельность стран – союзников СССР в ходе Второй мировой войны.

Продолжительность занятия – 4 ч.

Практическое занятие 6.

Вид практического занятия: доклад в форме презентации

Тема 6. Организация защиты информации в послевоенный период.

Содержание практического занятия:

Учебные вопросы.

1. Совершенствование системы защиты государственных секретов во второй половине 40-х – первой половине 50-х годов.
2. Организация защиты государственных секретов во второй половине 50-х и в 60-е годы.
3. Обеспечение защиты информации в 70-80-е годы в нашей стране.

Продолжительность занятия – 4 ч.

Практическое занятие 7.

Вид практического занятия: смешанная форма практического занятия.

Тема 7. Основные особенности организации защиты информации на современном этапе.

Содержание практического занятия:

Учебные вопросы.

1. Полномочия органов власти, специальных федеральных органов и предприятий в области защиты информации.
2. Информационная асимметрия и информационное доминирование в современном мире.
3. Государственная политика в области защиты информации: обеспечение преемственности и новые аспекты её реализации.
4. Характеристика концепции информационного сдерживания.

Продолжительность занятия – 4 ч.

Практическое занятие 8.

Вид практического занятия: смешанная форма практического занятия.

Тема 8. Современное состояние системы защиты информации и перспективы её совершенствования.

Содержание практического занятия:

Учебные вопросы.

1. Недостатки в системе защиты информации и их основные причины.
2. Основные направления разработки правовых и организационных основ деятельности подразделений защиты информации.
3. Основные перспективы развития системы защиты информации.

Продолжительность занятия – 4 ч.

Практическое занятие 9.

Вид практического занятия: смешанная форма практического занятия.

Тема 9. Операции информационного противоборства в контексте международного права.

Содержание практического занятия:

Учебные вопросы.

1. Характеристика подзаконных нормативных документов по защите информации.
2. Обзор международных правовых документов, регулирующих права и свободы граждан в информационной сфере.
3. Анализ международных правовых соглашений в области предупреждения и пресечения информационно-психологической агрессии.

Продолжительность занятия – 4 ч.

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом

4. Указания по проведению самостоятельной работы студентов

№ п / п	Тема для самостоятельного изучения	Вопросы для самостоятельной работы	Литература по теме	Кол-во часов
				Очное обучение
1	Средства информации в Первой и Второй мировой войне, механизмы контроля и управления.	<ol style="list-style-type: none">1. Взаимоотношения прессы и военной тайны, деятельность русской военной цензуры.2. Какова была эффективность воздействия печати, объекты, задачи, руководство, организация пропаганды и тайных операций?3. Что показал опыт войн, положительные и отрицательные	Волковский Н.Л. История информационных войн. Ч. 2 - СПб.: Полигон 2003 г., с.10-115 и др.	15

		моменты информационного противоборства, роль дезинформации, лжи, фальсификации в достижении целей противоборства?		
2	Охота за «Энигмой» в огне Второй мировой войны.	<p>1. Особенности появления и распространения «Энигмы» как машины для шифрования сообщений.</p> <p>2. Деятельность иностранных спецслужб по раскрытию кодов «Энигмы», опыт проведения спецопераций и основные уроки криптографического противоборства.</p> <p>3. Исторический опыт сотрудничества спецслужб СССР и западных союзников в области тайных операций Второй мировой войны.</p>	<p>Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций. - Москва: «Гелиос АРВ» 2008 г., с167-219 и др.</p>	15
3	Исторические особенности информационного обеспечения советских и российских войск в локальных войнах и вооруженных конфликтах второй половины XX-го – начала XXI-го века.	<p>1.Руководство информационно-психологическим обеспечением конфликтов.</p> <p>2. Организация информационно-психологических действий в ходе операций в конфликтах.</p> <p>3. Опыт освещения конфликтов в свете мнения средств массовой информации.</p>	<p>Волковский Н.Л. История информационных войн. Ч. 2 - СПб.: Полигон 2003 г., с.509-625 и др.</p>	15
4	Основные перспективы развития государственной информационной политики в XXI веке.	<p>1. Исторический очерк развития государственной информационной политики в нашей стране.</p> <p>2. Основные первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности России.</p> <p>3. Основные направления совершенствования государственной информационной политики Российской Федерации.</p>	<p>Белов Е. Б., Лось В.П., Мещеряков Р.В., Шелупанов А. А. Основы информационной безопасности. Учебное пособие. М., «Горячая линия - Телеком», 2006 г., с. 20 – 44 и др.</p>	15
Всего:				60

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Анисимов А.А. Менеджмент в сфере информационной безопасности. Учебное пособие. – М.: Интернет – Университет информационных технологий / БИНОМ. Лаборатория знаний, 2010.
2. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность. Учебное пособие. – М.: «ФОРУМ», 2011.
3. Воронов А.Н. История и современная система защиты информации в России. Учебное пособие. – Королёв МО: КИУЭС, 2011.

Дополнительная литература:

1. Воронцова Л. В., Фролов Д. Б. История и современность информационного противоборства. М.: «Горячая линия – Телеком», 2006.
2. Волконский Н. Л. История информационных войн. Части I, II. – СПб.: ООО «Издательство – Полигон», 2003.
3. Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций. М.: «Гелиос АРВ», 2008.

Рекомендуемая литература:

1. Белов Е. Б., Лось В.П., Мещеряков Р.В., Шелупанов А. А. Основы информационной безопасности. Учебное пособие. М.: «Горячая линия – Телеком», 2006.
2. Вепринцев В. Б., Манойло А. В., Петренко А. И., Фролов Д. Б. Операции информационно - психологической войны. Краткий энциклопедический словарь-справочник. М.: «Горячая линия – Телеком», 2005.
3. Тихонов В. А., Райх В. В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. Учебное пособие. М.: «Гелиос АРВ», 2006.
4. Потапов В. В. Тайная история России. М.: «Мартин», 2008.

7. Перечень ресурсов информационно – телекоммуникационной сети «Интернет»

1. <http://www.biblioclub.ru>
2. <http://znanium.com>
3. Энциклопедия информационной безопасности. – Публикации, статьи

www.wikIsec.ru).

8. Перечень информационных технологий

Перечень программного обеспечения:

MS Office, PowerPoint.

Информационные справочные системы:

1. Учебный портал с электронно-методическими комплексами (do.kimes).
2. Универсальная библиотека онлайн (www.biblioclub.ru).
3. Polpred.com (www.polpred.com).
4. Единое окно доступа (www.window.edu.ru).
5. Издательский дом «Гребенников» (<http://grebennikov.ru/>).
6. ЭБС «Рукопт» (www.rucont.ru).
7. Электронные книги: электронная библиотека пособий на компакт дисках. ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348.