МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Шуйский филиал ИвГУ

Кафедра математики, информатики и методики обучения

ОДОБРЕНО:
Руководитель ОП
_____ С.А. Зайцева
(подпись)
«25» февраля 2025 г.

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Уровень высшего образования:	магистратура
Квалификация выпускника:	магистр
Направление подготовки:	44.04.01 Педагогическое образование
Направленность (профиль) образовательной программы:	Информационные технологии в профессиональной деятельности

Шуя

1. Цели освоения дисциплины: развитие профессиональной компетентности студентов в сфере информационных технологий, расширение общетехнического кругозора, содействие пониманию защиты информации как комплекса целенаправленных процессов обеспечения информационной безопасности, формирование представлений о современном содержании и перспективах совершенствования защиты информации в условиях образовательного процесса.

2. Место дисциплины в структуре ОП

Дисциплина является обязательной для изучения; относится к формируемой участниками образовательных отношений части блока дисциплин Б1, входит в модуль «Прикладные информационные технологии в образовании».

Успешное освоение данной дисциплины будет способствовать готовности обучающихся к освоению дисциплин: «Цифровые технологии в управлении образовательным учреждением», «Информационно-коммуникационная компетентность личности в условиях цифровой трансформации образования», «Облачные технологии в профессиональной деятельности», «Информационные технологии контроля и оценки учебных достижений», «Проектирование и реализация дистанционных образовательных курсов», «Теория и методика электронного обучения», «Проектирование и разработка Web-портфолио», успешному прохождению производственной практики (научно-исследовательской работа), производственной практики (педагогической практики), подготовке к сдаче и сдаче государственного экзамена, выполнению и защите выпускной квалификационной работы.

Студент, приступающий к изучению дисциплины, должен обладать знаниями, умениями, навыками, полученными ранее в ходе обучения на уровне бакалавриата.

Знать:

− методы критического анализа и оценки проблемных ситуаций на основе системного подхода;

− стандартные программно-аппаратные средства реализации информационных процессов.

Уметь:

− оценивать пригодность и качество образовательных ресурсов для организации учебно-воспитательного процесса;

– оценивать эффективность организации межличностного взаимодействия в современном информационном пространстве;

− осуществлять ауди, видео, текстовую коммуникацию (двусторонняя связь, конференция, мгновенные и отложенные сообщения, автоматизированные коррекция текста и перевод между языками).

Владеть:

− методами работы со стандартами и прикладными программами общего и специального назначения для организации собственной учебной деятельности;

− опытом организации сетевого взаимодействия в условиях современного информационного пространства.

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

3.1. Компетенции, формированию которых способствует данная дисциплина

При реализации дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

а) универсальные компетенции (УК) и индикаторы их достижения:

–

б) общепрофессиональные компетенции (ОПК) и индикаторы их достижения:

–

в) профессиональные компетенции (ОПК) и индикаторы их достижения:

Код и наименование профессиональной компетенции выпускника	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)
Тип задач профессиональной деятельности: педагогический		
ПК-1. Способен применять средства информационно-коммуникационных технологий в решении педагогических задач.	ПК-1.1. Знает: основы методики преподавания с использованием дистанционных образовательных технологий и электронного обучения. ПК-1.2. Умеет: адекватно оценивать портфель образовательных ИКТ-решений для учебного процесса; эффективно использовать стандартные компьютерные приложения и интегрировать современные ИКТ в образовательный процесс; выявлять и внедрять ИКТ-инновации в образовательный процесс. ПК-1.3. Владеет: методиками организации и осуществления образовательного процесса с использованием ИКТ; современными ИКТ, необходимыми для построения эффективных коммуникаций между участниками образовательного процесса; методами анализа эффективности использования ИКТ в образовательном процессе.	Профессиональный стандарт 01.001 «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)».
ПК-2. Способен разрабатывать электронные ресурсы для организации учебно-воспитательного процесса.	ПК-2.1. Знает: нормы законодательства РФ, регламентирующие использование ИКТ и электронного обучения при реализации основных и дополнительных образовательных программ; требования к использованию ИКТ-методов, инструментов и технологий для создания электронных образовательных ресурсов (ЭОР). ПК-2.2. Умеет: рецензировать ИКТ-решения для создания ЭОР на соответствие психолого-педагогическим требованиям; успешно организовывать работу по созданию и редактированию образовательного контента. ПК-2.3. Владеет методами поиска, управления и представления информации, необходимой для эффективного выполнения профессиональных задач в электронной информационно-образовательной среде; технологиями разработки ЭОР – элементов электронной информационно-образовательной среды.	Профессиональный стандарт 01.001 «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)».

3.2. Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения формируемых компетенций

В результате освоения дисциплины обучающийся должен:

Знать:

– программно-аппаратные средства реализации ИКТ в педагогическом процессе (ПК-1 (индикаторы – 1, 2, 3);

– нормы законодательства РФ, регламентирующие использование ЭОР в учебно-воспитательном процессе ИКТ (ПК-2 (индикаторы – 1, 2, 3).

Уметь:

– оценивать пригодность и качество образовательных ресурсов для организации учебно-воспитательного процесса (ПК-1 (индикаторы – 1, 2, 3);

– создавать самостоятельно и успешно организовывать работу коллектива по созданию и редактированию образовательного контента (ПК-2 (индикаторы – 1, 2, 3).

Владеть:

– методами анализа эффективности использования ИКТ в образовательном процессе (ПК-1 (индикаторы – 1, 2, 3);

– навыками оценки качества ЭОР (ПК-2 (индикаторы – 1, 2, 3);

– методами организации информационной безопасности при осуществлении поиска и использования программных продуктов и сред, предназначенных для разработки ЭОР (ПК-2 (индикаторы – 1, 2, 3).

4. Объём и содержание дисциплины

Очная форма обучения

Объём дисциплины составляет 2 зачётных единицы (54 час.)

Контактная работа 24,25 час.

Самостоятельная работа 29,75 час.

Виды учебных занятий и формы промежуточной аттестации	1 сем.	
	Контактная работа с преподавателем	Самостоятельная работа обучающегося
Лекции	12	29,75
Практические занятия	12	
Зачет	0,25	-
Всего	24,25	29,75

Заочная форма обучения

Объём дисциплины составляет 2 зачётных единицы (54 час.)

Контактная работа 6,25 час.

Самостоятельная работа 47,75 час.

Виды учебных занятий и формы промежуточной аттестации	1 курс	
	Контактная работа с преподавателем	Самостоятельная работа обучающегося
Лекции	3	45
Практические занятия	3	
Зачет	0,25	2,75

Всего	6,25	47,75

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и объемом учебных занятий

Очная форма обучения

№ п/п	Раздел (тема) дисциплины	Семестр	Виды учебных занятий, включая самостоятельную работу обучающихся и объем (в часах)				Формы текущего контроля успеваемости Формы промежуточной аттестации
			Занятия лекционного типа	Занятия семинарского типа		Самостоятельная работа	
				Лаб.	Пр.		
1.	Спектр информационных угроз: эволюционное изменения, текущее состояние, тенденции.	1	4		4	10	практические задания, микроисследование, доклад
2.	Динамичная актуализация законодательной базы как основа эффективной организации информационной безопасности в современных условиях.	1	4		4	10	практические задания, микроисследование, доклад
3.	Современные организационные и технические средства обеспечения информационной безопасности.	1	4		4	9,75	практические задания, микроисследование, доклад
ИТОГО			12		12	29,75	Зачет

Заочная форма обучения

№ п/п	Раздел (тема) дисциплины	Курс	Виды учебных занятий, включая самостоятельную работу обучающихся и объем (в часах)				Формы текущего контроля успеваемости Формы промежуточной аттестации
			Занятия лекционного типа	Занятия семинарского типа		Самостоятельная работа	
				Лаб.	Пр.		
1	Спектр информационных угроз: эволюционное изменения, текущее состояние, тенденции.	1	1,5		-	15	практические задания, микроисследование, доклад
2.	Динамичная актуализация законодательной базы как основа эффективной организации информационной безопасности в современных условиях.	1	1,5		-	15	практические задания, микроисследование, доклад
3.	Современные организационные и технические средства обеспечения информационной безопасности.	1	-		3	15	практические задания, микроисследование, доклад
ИТОГО			3		3	45	Зачет

4.2. Развернутое описание содержания учебного материала по разделам (темам)

Тема 1. Спектр информационных угроз: эволюционное изменения, текущее состояние, тенденции.

Актуальная терминология в области защиты информации; ретроспектива угроз информационной безопасности в контексте развития компьютерных и коммуникационных технологий; специфика современного состояния защищённости информационной среды на уровнях унитарной компьютерной системы, локальной сети, сети Интернет; угрозы информационной безопасности, обусловленные социальными и психологическими факторами; современные источники информационных угроз, количественный и качественный (квалификационный) рост целенаправленной преступности в области компьютерных систем и технологий; перспективные технологические решения, потенциально повышающие уязвимость информационных систем и возможные меры противодействия.

Тема 2. Динамичная актуализация законодательной базы как основа эффективной организации информационной безопасности в современных условиях.

Законодательный уровень обеспечения информационной безопасности; документальная основа информационной безопасности в Российской Федерации; организация законотворческой деятельности в области защиты информации; подзаконные акты; Доктрина информационной безопасности Российской Федерации (ред. 2016 г.) – интегральная основа формирования государственной политики обеспечения информационной безопасности; принципы построения законодательных систем защиты информации в развитых государствах: особенности, достоинства и недостатки; интеграция Российской Федерации в международную систему обеспечения информационной безопасности.

Тема 3. Современные организационные и технические средства обеспечения информационной безопасности.

Государственные органы Российской Федерации, обеспечивающие защиту информационных ресурсов: законодательная основа деятельности, разделение компетенций, сотрудничество и кооперация; мировой и российский рынки аппаратных и программных средств обеспечения информационной безопасности; перспективные технологические решения в области защиты информации; процедуры формирования безопасной информационной среды в структуре профессиональной деятельности; критерии обеспечения заданного уровня информационной безопасности – действующие стандарты, эмпирические и нормативные форматы.

5. Образовательные технологии, в том числе перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

В программе дисциплины предусмотрено использование в учебном процессе активных и интерактивных форм проведения занятий (дискуссий, разбор конкретных ситуаций и др.). Эти технологии в сочетании с внеаудиторной работой решают задачи формирования и развития профессиональных умений и навыков обучающихся, как основы профессиональной компетентности в сфере информационных технологий в образовании.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: технологии смешанного обучения, мультимедиа технологии, технологии визуализации.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся по дисциплине осуществляется в следующих формах:

- конспектирование и реферирование источников по тематике учебного курса;
- подготовка доклада по вопросам организации информационной безопасности участников образовательного процесса;
- выполнение практических заданий по в организации информационной безопасности образовательного учреждения;
- исполнение самостоятельных проектных работ (микроисследований).

Полностью весь методический материал по обеспечению самостоятельной работы студентов приводится в приложении 1 к настоящей программе. Доступ к методическим материалам осуществляется через сайт Шуйского филиала ИвГУ, в том числе через ЭБС Шуйского филиала ИвГУ на платформе «Руконт» информационную среду кафедры Математики, информатики и методики обучения, реализованную посредством приложения ClassRoome сервиса Google в домене Шуйского филиала ИвГУ (sspu.ru).

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине

Для текущего контроля успеваемости применяются:

- исполнение практических заданий в ходе аудиторного взаимодействия на практических занятиях – 7 заданий по 5 баллов / максимально 35 баллов;
- исполнение самостоятельных работ (микроисследований) в процессе сетевого / дистанционного взаимодействия – 3 работы по 5 баллов / максимально 15 баллов;
- подготовка докладов – 3 доклада по 5 баллов / максимально 15 баллов.

Помимо этого учитывается:

- степень участия обучающегося в коллективных обсуждениях – 5 баллов,

На зачете по дисциплине «Информационная безопасность и защита информации» оцениваются контролируемые знания, умения и владения, характеризующие этапы формирования компетенций в процессе освоения образовательной программы. Зачет проводится в форме тестирования (до 30 баллов).

Общая накопительная оценка складывается из баллов текущей успеваемости в семестре по предмету и баллов, полученных студентами на зачете.

Оценка на зачете выставляется по следующей шкале:

Шкала оценки результатов по дисциплине
«Информационная безопасность и защита информации»

Повышенный уровень	Базовый уровень	Пороговый уровень	Ниже порогового уровня
зачтено	зачтено	зачтено	не зачтено
85-100 баллов	71-84 балла	61-70 баллов	60 и менее баллов

Фонд оценочных средств по дисциплине «Информационная безопасность и защита информации» в полном объёме представлен в Приложении 2 к рабочей программе.

8. Учебно-методическое и информационное обеспечение дисциплины

Учебная и учебно-методическая литература:

- ***основная литература:***

1. Вострецова, Е. В. Основы информационной безопасности : учебное пособие / Е. В. Вострецова ; Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. – Екатеринбург : Издательство Уральского университета, 2019. – 207 с. :

ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=697636 . – Библиогр. в кн. – ISBN 978-5-7996-2677-8. – Текст : электронный.
2. Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 . – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.
3. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.

- ***дополнительная литература:***

1. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605
2. Гашков, С. Б. Криптографические методы защиты информации : учебное пособие для студентов вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - Москва : Академия, 2010. - 304 с.
3. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557
4. Информационная безопасность : учебно-методические материалы для проведения практических занятий / Министерство образования и науки РФ; ГОУ ВПО "Шуйский государственный педагогический университет" ; авт.-сост. А. А. Михайлов, Г. Д. Хубулов. - Шуя : Изд-во ГОУ ВПО "ШГПУ", 2010. - 56 с.
5. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726. – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.
6. Петров, С. В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.
7. Попов, В. Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности : учебное пособие / В. Б. Попов. - Москва : Финансы и статистика, 2005. - 176 с.
8. Расторгуев, С. П. Основы информационной безопасности : учебное пособие для студентов высших учебных заведений / С. П. Расторгуев. - Москва : Академия, 2007. - 192 с.

Интернет-ресурсы:

1. Обзоры, аналитика, тестирование компьютерных систем, информационной техники и программного обеспечения www.ixbt.com

2. Компьютерра-Онлайн www.computerra.ru

Современные профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн»;
Коллекция Шуйского филиала ИвГУ на национальном цифровом ресурсе «Руконт»;
Консультант Плюс http://www.consultant.ru/
Методическое хранилище Ивановского института развития образования].- http://www.iroio.ru/;
Словари и энциклопедии на Академике. - https://dic.academic.ru/;
Статистические материалы региональных исследований в области общего образования. - http://www.ivege.ru/content/work/katestvo/region_monitoring.

Программное обеспечение:

В процессе изучения дисциплины используются офисные пакеты Microsoft Office, Open Office, программа для просмотра и чтения файлов PDF Adobe Acrobat Reader DC, программа для воспроизведения флэш-анимации в браузерах Adobe Flash Player, вэб-обозреватели Google Chrome, Opera, Антивирус Касперского; 1С университет, Google-диск: https://drive.google.com; Google-документы: https://docs.google.com; сборник тестирующих и диагностирующих программ 2k10 (обновляемый), программный пакет организации документооборота Libre Office.

9. Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного типа, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории.
2. Учебная аудитория для проведения занятий семинарского типа, укомплектованная специализированной мебелью и техническими средствами обучения.
3. Учебная аудитория для проведения текущего контроля и промежуточной аттестации, укомплектованная специализированной мебелью и техническими средствами обучения.
4. Помещение для самостоятельной работы, оснащенное специализированной мебелью, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.
5. Учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации: презентации, видео-ролики.

Автор рабочей программы дисциплины: В.В. Иванов, доцент кафедры математики, информатики и методики обучения, кандидат технических наук, доцент.

Программа рассмотрена на заседании кафедры математики, информатики и методики обучения «19» февраля 2025 г., протокол № 8

Программа обновлена
протокол заседания кафедры № ___ от «___» _____ 20___ г.
Согласовано:
Руководитель ОП
_____ С.А. Зайцева
(подпись)

Программа обновлена
протокол заседания кафедры № ___ от «___» _____ 20___ г.
Согласовано:
Руководитель ОП
_____ С.А. Зайцева

Программа обновлена
протокол заседания кафедры № ___ от «___» _____ 20___ г.
Согласовано:
Руководитель ОП
_____ С.А. Зайцева
(подпись)

Программа обновлена
протокол заседания кафедры № ___ от «___» _____ 20___ г.
Согласовано:
Руководитель ОП
_____ С.А. Зайцева
(подпись)

Приложение 1.

Методические указания для обучающихся по освоению дисциплины

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

Практическое задание (всего 7 заданий), максимальная оценка 5 баллов за 1 выполненное задание.

Задание:

Выполнить практическое задание по контролируемой теме; на практических занятиях предполагается использование компьютерных информационных средств – как для поиска необходимой информации, так и как объекта и/или инструмента исследования.

Критерии оценки

Оценки в баллах	Критерии
3	Правильное выполнение задания в полном объеме
1	Аккуратность и грамотность в оформлении результатов
1	Целесообразная оригинальность, дополнительные соображения и т.п.
5	МАКСИМАЛЬНАЯ ОЦЕНКА

Тема 1. Спектр информационных угроз: эволюционное изменения, текущее состояние, тенденции

Практическое задание №1

Вопросы для изучения:

1) Актуальная терминология в области защиты информации.
2) Ретроспектива угроз информационной безопасности в контексте развития компьютерных и коммуникационных технологий.
3) Специфика современного состояния защищенности информационной среды на уровнях унитарной компьютерной системы, локальной сети, сети Интернет.

Практическое задание:

1) Составить структурированный словарь актуальных понятий в области обеспечения информационной безопасности.
2) Построить хронологическую последовательность (от разработки первых ЭВМ до настоящего времени) угроз информационной безопасности: их возникновение, проявление до уровня значимой общественной опасности и возможное снятие актуальности. Соотнести хронологию информационных угроз с внедрением глобальных технологических решений (появление персональных компьютеров, широкое гражданское применение Интернета, распространение мобильных информационных устройств и др.).
3) Подготовить краткое эссе, представляющее специфику современного состояния защищённости информационной среды на уровнях а) унитарной компьютерной системы, б) локальной компьютерной сети, в) сети Интернет.

Результат выполнения задания представить в виде файла оптимального формата; отправить результирующий файл на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер практического занятия (сквозная нумерация по учебной дисциплине), например:
ФТЭС1-3_ БорисовББ_прзан1

Практическое задание №2

Вопросы для изучения:

1) Спектр угроз информационной безопасности; информационные угрозы, обусловленные социальными и психологическими факторами.

2) Современные источники информационных угроз, количественный и качественный (квалификационный) рост целенаправленной преступности в области компьютерных систем и технологий.
3) Перспективные технологические решения, потенциально повышающие уязвимость информационных систем и возможные меры противодействия им.

Практическое задание:

1) Подготовить краткое эссе, представляющее овладение обучающимся ключевыми положениями изученных вопросов.

Результат выполнения задания представить в виде файла оптимального формата; отправить результирующий файл на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер практического занятия (сквозная нумерация по учебной дисциплине), например:
ФТЭС1-3_ БорисовББ_прзан1

Тема 2. Динамичная актуализация законодательной базы как основа эффективной организации информационной безопасности в современных условиях.

Практическое задание №3

Вопросы для изучения:

1) Законодательный уровень обеспечения информационной безопасности; документальная основа информационной безопасности в Российской Федерации; организация законотворческой деятельности в области защиты информации; подзаконные акты.
2) Доктрина информационной безопасности Российской Федерации (ред. 2016 г.) – интегральная основа формирования государственной политики обеспечения информационной безопасности.

Практическое задание:

1) Подготовить краткое эссе, представляющее овладение обучающимся ключевыми положениями изученных вопросов.

Результат выполнения задания представить в виде файла оптимального формата; отправить результирующий файл на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер практического занятия (сквозная нумерация по учебной дисциплине), например:
ФТЭС1-3_ БорисовББ_прзан1

Практическое задание №4

Вопросы для изучения:

1) Принципы построения законодательных систем защиты информации в развитых государствах: особенности, достоинства и недостатки.
2) Интеграция Российской Федерации в международную систему обеспечения информационной безопасности.

Практическое задание:

1) Подготовить информационное сообщение об особенностях построения и функционирования законодательства в области информационной безопасности для одного из государств по выбору преподавателя.
2) Подготовить краткое эссе, представляющее овладение обучающимся ключевыми положениями изученного вопроса №2.

Результат выполнения задания представить в виде файла оптимального формата; отправить результирующий файл на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер практического занятия (сквозная нумерация по учебной дисциплине), например:
ФТЭС1-3_ БорисовББ_прзан1

Тема 3. Современные организационные и технические средства обеспечения информационной безопасности.

Практическое задание №5

Вопросы для изучения:

1) Государственные органы Российской Федерации, обеспечивающие защиту информационных ресурсов: законодательная основа деятельности, разделение компетенций, сотрудничество и кооперация.

Практическое задание:

1) Преподаватель выбирает для углубленного ознакомления 1 или 2 организации из нижеприведенного списка:
   - Комитет Государственной думы по безопасности и противодействию коррупции
   - Совет безопасности России
   - Служба внешней разведки Российской Федерации (СВР России)
   - Министерство обороны Российской Федерации (Минобороны России)
   - Министерство внутренних дел Российской Федерации (МВД России)
   - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

   Студент должен для каждой выбранной организации найти с использованием публичных информационных источников следующие данные:
   - дата создания
   - вышестоящий государственный орган и/или должностное лицо
   - действующий руководитель
   - количество сотрудников (ориентировочно)
   - годовой бюджет
   - официальный сайт
   - декларируемые задачи в области защиты информации
   - конкретные действия в области защиты информации в последние годы (2...3 действия)

Результат выполнения задания представить в виде файла оптимального формата; отправить результирующий файл на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер практического занятия (сквозная нумерация по учебной дисциплине), например:
ФТЭС1-3_ БорисовББ_прзан1

Практическое задание №6

Вопросы для изучения:

1) Мировой и российский рынки аппаратных и программных средств обеспечения информационной безопасности
2) Перспективные технологические решения в области защиты информации

Практическое задание:

1) Подготовить информационное сообщение об одном из ведущих разработчиков / производителей средств защиты информации (приоритетные направления деятельности, ключевые технологические решения, доли рынков и проч.). Студент может по согласованию с преподавателем самостоятельно выбрать объект изучения, отдавая предпочтение российским компаниям или зарубежным организациям, осуществляющим масштабную плодотворную деятельность в Российской Федерации.
2) Подготовить краткое эссе на тему «Это будет революцией» об одном из перспективных средств защиты информации (алгоритм, прототипы программных и аппаратных продуктов); обосновать значение рассматриваемого средства для существенного

повышения защищённости информационных ресурсов в ближайшем будущем.
Результат выполнения задания представить в виде файла оптимального формата; отправить результирующий файл на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер практического занятия (сквозная нумерация по учебной дисциплине), например:
ФТЭС1-3_ БорисовББ_прзан1

Практическое задание №7

Вопросы для изучения:
1) Процедуры формирования безопасной информационной среды в структуре профессиональной деятельности.
2) Критерии обеспечения заданного уровня информационной безопасности.

Практическое задание:
1) Составить аннотированный перечень аппаратных и программных средств информационной защиты, реализованных в информационной системе, применяемой студентом (например, перечислить средства защиты домашней компьютерной сети или рабочего компьютера, подключенный к корпоративной локальной сети / сети Интернет).
2) Подготовить краткое сообщение об одном из действующих стандартов классификации по уровню информационной защищённости компьютерных и коммуникационных систем.

Результат выполнения задания представить в виде файла оптимального формата; отправить результирующий файл на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер практического занятия (сквозная нумерация по учебной дисциплине), например:
ФТЭС1-3_ БорисовББ_прзан1

ПРИМЕРНАЯ ТЕМАТИКА МИКРОИССЛЕДОВАНИЙ

Задание: Выполнить самостоятельную проектную работу (микроисследование) по контролируемой теме. Всего необходимо выполнить 3 работы, максимальная оценка 5 баллов за 1 выполненную работу.

Критерии оценки

Оценки в баллах	Критерии
2	Самостоятельность в подготовке материала
1	Аргументированность и полнота материала
1	Актуальность использованных информационных источников
1	Качество презентации
5	МАКСИМАЛЬНАЯ ОЦЕНКА

Тематика микроисследований

1. Свободные и условно-бесплатные программные инструменты для оценки уязвимостей WiFi-сети (сравнительный обзор).
2. Организация эффективной и безопасной многопользовательской работы на учебных компьютерах.
3. Программные средства для восстановления информации на магнитных дисках, файловая система которых повреждена в результате целенаправленного деструктивного воздействия (сравнительный обзор).
4. Свободные и условно-бесплатные антивирусные средства: оценка потребительских качеств и пригодности к эффективному применению начинающими / неквалифицированными пользователями.

5. Программные средства для поддержания оптимальной рабочей среды пользователя и противодействия попыткам её искажения.
6. Программные инструменты для выявления и устранения вредоносного программного обеспечения (malware).
7. Оптимизирующая настройка встроенных средств безопасности операционных систем семейства Windows.
8. Оптимизирующая настройка встроенных средств безопасности операционных систем семейства Android.
9. «Гражданские» общедоступные средства шифрования конфиденциальной информации.
10. Свободные и условно-бесплатные средства верификации подлинности контента.

ДОКЛАДЫ

Задание: Подготовить доклад по контролируемой теме. Тематика актуализируется в соответствии с трендами развития информационных технологий. Всего необходимо подготовить 3 доклада, максимальная оценка 5 баллов за 1 подготовленный доклад. Доклад презентуется на аудиторном занятии.

Критерии оценки

Оценки в баллах	Критерии
2	Самостоятельность в подготовке материала
1	Аргументированность и полнота материала
1	Актуальность использованных информационных источников
1	Качество презентации
5	МАКСИМАЛЬНАЯ ОЦЕНКА

Примерная тематика докладов

1. Лицензионная политика российских производителей антивирусных программных средств (на примере АО «Лаборатория Касперского» и ООО «Доктор Веб» или иных отечественных разработчиков / производителей по выбору студента (не менее 2)).
2. Альтернативные операционные системы для образовательных учреждений: преимущества в информационной безопасности.
3. Использование социальных сетей для формирования заданного общественного мнения.
4. Российская система защиты персональных данных.
5. Формирование современной структуры государственных органов Российской Федерации, обеспечивающих информационную безопасность.
6. Организация разграничения прав доступа к информации и обнаружения НСД в образовательных учреждениях.
7. Обеспечение бесперебойного функционирования корневых серверов DNS.
8. Возможности и перспективы информационного противодействия сетевым террористическим структурам.
9. Значение международной стандартизации методов и процедур защиты информации.
10. Современные средства авторизации доступа к информационным ресурсам.