Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования
«Полоцкий государственный университет
имени Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«27» 06. 2025 г.
Регистрационный № УД – 500/25 /уч.

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Учебная программа учреждения образования
по учебной дисциплине для специальности
1-23 01 02 «Лингвистическое обеспечение межкультурных коммуникаций»

2025 г.

Учебная программа составлена на основе на основе образовательного стандарта по специальности высшего образования ОСВО 1–23 01 02-2021 и учебного плана по специальности 1-23 01 02 «Лингвистическое обеспечение межкультурных коммуникаций», направление специальности 1-23 01 02-01 «Лингвистическое обеспечение межкультурных коммуникаций (информационное обслуживание)». Регистрационный № 18-1-21/уч. ГФ от 26.07.2021 для дневной формы получения образования.

СОСТАВИТЕЛЬ:
Валерий Михайлович Чертков, канд. техн. наук, доцент, доцент кафедры технологий программирования учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой технологий программирования учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 5 от «30» 05 2025 г.);

Научно-методическим советом учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 7 от «27» 06 2025 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Интенсивное внедрение информационных технологий во все области деятельности человека позволяет обеспечить оперативный обмен сведениями между службами, отделами предприятия и организациями в целом за счет оптимизации информационных потоков, что позволяет ускорить и сделать более качественным процесс их взаимодействия. Сведения, которыми обмениваются такие партнеры, как правило, носят конфиденциальный характер и относятся к категориям служебной или государственной тайны, что требует подготовки современных специалистов, обладающих не только специальными знаниями по их профилю обучения, но и владением основами защиты информации.

Цель изучения дисциплины: получение базовых знаний по вопросам обеспечения информационной безопасности в условиях различных по виду, происхождению и характеру возникновения угроз.

Задачи изучения дисциплины:

– изучение угроз информационной безопасности;

– изучение методов и средств защиты информации;

– изучение алгоритмов и методов криптографического шифрования;

– изучение теоретических основ информации;

– приобретение навыков по криптографическому шифрованию информации.

Требования к уровню освоения содержания учебной дисциплины

Освоение учебной дисциплины должно формировать у студента следующую **специализированную компетенцию:** оценивать эффективность функционирования механизмов контроля информационных рисков.

В результате изучения дисциплины «Управление информационной безопасностью» обучаемый должен:

знать:

– системную методологию и правовое обеспечение защиты информации;

– основы криптографической защиты информации;

– особенности защиты информации в информационных системах;

– приоритеты развития информационных технологий, повышающих эффективность защиты информационного пространства Союзного государства Беларуси и России в современных условиях;

– методы получения простых больших чисел;

уметь:

– определять возможные каналы утечки информации и обоснованно выбирать средства их блокирования;

– разрабатывать рекомендации по защите объектов различного типа от несанкционированного доступа;

– реализовывать алгоритмы эффективного кодирования для уменьшения объема хранимой и передаваемой информации;

– реализовывать криптографические алгоритмы для защиты информации от несанкционированного доступа;

владеть:

– основными приемами анализа вероятных угроз информационной безопасности для заданных объектов;

– навыками применения положений теории информации для криптографического преобразования информации.

Связи с другими учебными дисциплинами

Базовой учебной дисциплиной по учебной дисциплине «Управление информационной безопасностью» являются «Основы управления интеллектуальной собственностью». В свою очередь учебная дисциплина «Управление информационной безопасностью» является базовой для дипломного проектирования.

В соответствии с учебным планом программа предусматривает для изучения дисциплины следующее распределение учебных часов:

Форма получения высшего образования	дневная
Курс	5
Семестр	9
Всего учебных часов по дисциплине	108
Всего аудиторных часов по дисциплине	40
В том числе:	
Лекции, часов	20
Практические занятия, часов	20
Самостоятельная работа, часов	68
Форма промежуточной аттестации	зачет
Трудоемкость дисциплины, з.е.	3

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

ВВЕДЕНИЕ В ДИСЦИПЛИНУ

Тема 1. Введение в дисциплину

Цели и задачи изучения дисциплины. Основные проблемы информационной безопасности. Законодательство РБ в области ЗИ. Приоритетные направления в РБ в области защиты информации.

Государственные органы и учреждения, занимающиеся вопросами защиты информации в РБ: Министерство связи и информатизации Республики Беларусь, Оперативно-аналитический центр при Президенте Республики Беларусь, Научно-исследовательский институт технической защиты информации, Национальный центр интеллектуальной собственности, Государственный комитет по стандартизации Республики Беларусь, Белорусский государственный институт стандартизации и сертификации.

РАЗДЕЛ 1. ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 2. Основные понятия информационной безопасности и защиты информации

Защита информации. Объект защиты. Цель защиты информации. Эффективность защиты информации. Защита информации от утечки. Защита информации от несанкционированного воздействия. Защита информации от непреднамеренного воздействия. Защита информации от разглашения. Защита информации от несанкционированного доступа. Система защиты информации. Автоматизированная информационная система. Конфиденциальность данных. Целостность информации. Достоверность информации. Доступность данных. Политика безопасности.

Тема 3. Анализ угроз информационной безопасности

Классификация угроз информационной безопасности. Преднамеренные и непреднамеренные угрозы ИБ. Гипотетическая модель потенциального нарушителя. Незаконное использование привилегий. Вредоносные программы. Уровни доступа. Основные методы реализации угроз ИБ.

Характерные особенности сетевых атак. Цели потенциального нарушителя. Категории сетевых атак. Атаки доступа. Атаки модификации. Атаки типа «отказ в обслуживании». Комбинированные атаки. Угрозы и уязвимости беспроводных сетей. Рейтинг угроз ИБ. Анализ мнений экспертов и аналитиков.

РАЗДЕЛ 2. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 4. Правовое обеспечение защиты информации

Закон РБ от 6 сентября 1995 г. № 3850-XII «Об информатизации». Закон РБ от 29 ноября 1994 г. № 3411-XII «О государственных секретах». Закон РБ от 3 декабря 1997 г. № 102-З «Об органах государственной безопасности Республики Беларусь». Постановление Совета Министров РБ от 15 февраля 1999 г. № 237 «О служебной информации ограниченного распространения». Постановление Совета Министров РБ от 10 февраля 2000 г. № 186 «О некоторых мерах по защите информации в Республике Беларусь». Указ Президента Республики Беларусь от 12 мая 2004 г. № 231 «Вопросы Государственного центра безопасности информации при Президенте Республики Беларусь».

Тема 5. Виды компьютерных преступлений. Компьютерные вирусы

Правовая защита от компьютерных преступлений.

Примеры известных компьютерных преступлений. Виды компьютерных преступлений, мошенничество в интернете. Использование специальных программных средств мошенниками. Полезные советы по компьютерной безопасности.

Понятие вирус. История компьютерных вирусов. Классификация компьютерных вирусов. Особенности алгоритмов работы вирусов. Деструктивные возможности и пути проникновения вирусов. Методы защиты от вирусов.

РАЗДЕЛ 3. ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 6. Государственное регулирование в области защиты информации

Положения государственной политики информационной безопасности РБ. Система информационной безопасности РБ. Государственная система защиты РБ. Основные функции системы информационной безопасности. Мероприятия по защите информации.

Основные виды лицензируемой деятельности. Основные требования к организациям, претендующим на получение лицензий на работы в области защиты информации. Сертификация и аттестация средств защиты информации. Организационно-административные и организационно-технические методы защиты информации. Страхование как метод защиты информации.

Тема 7. Инженерно-техническая защита объектов от несанкционированного доступа

Классификация технических каналов утечки информации. Обзор технических средств негласного съема акустической информации. Технические средства защиты речевой информации. Звуковые сигналы

РАЗДЕЛ 4. ЭЛЕМЕНТЫ ТЕОРИИ СЛОЖНОСТИ. ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Тема 8. Количество информации. Энтропия

Определение количества информации. Энтропия ансамбля. Энтропия объединения. Свойства энтропии. Пространственная и временная сложность. Сложность проблем. Классы сложности и их характеристики. PN-полные и PN-сложные задачи.

РАЗДЕЛ 5. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Тема 9. Основные понятия криптографической защиты информации

Обобщенная схема криптосистемы шифрования. Шифр. Шифртекст. Ключ шифрования. Основные классы криптосистем. Классификации криптографических алгоритмов.

Схема симметричной и асимметричной криптосистем шифрования. Матрица ключей. Симметричный блочный шифр. Рассеивание. Перемешивание. Действия над числами. DES. 3-DES. Комбинирование блочных алгоритмов. Стандарт шифрования ГОСТ 28147-89. Табличные замены. Режим гаммирования. AES. IDEA. RC2. RC5. Blowfish. Основные режимы работы блочного симметричного алгоритма. RSA. Асимметричные криптосистемы на базе эллиптических кривых. ECES.

Тема 10. Функции хеширования и электронная цифровая подпись

Схема формирования хэша. Хэш-значение. Свойства функции хэширования. Стандарт хэширования ГОСТ Р 34.11-94. Основные процедуры цифровой подписи: процедура формирования, процедура проверки. DSA. ECDSA. ГОСТ Р 34.10-94. Стандарт цифровой подписи ГОСТ Р 34.10-2001. Управление криптоключами. Использование комбинированной криптосистемы. Метод распределения ключей Диффи-Хеллмана. Метод комплексной защиты конфиденциальности и аутентичности передаваемых данных. Протокол вычисления ключа парной связи ECKEP.

Учебно-методическая карта учебной дисциплины «Управление информационной безопасностью»
Дневная форма получения высшего образования

Номер раздела темы	Название раздела, темы	Количество аудиторных часов					Литература	Формы контроля знаний
		лекции	практические занятия	семинарские занятия	лабораторные занятия	управляемой самостоятельной работы студента		
	ВВЕДЕНИЕ В ДИСЦИПЛИНУ							
Тема 1.	Введение в дисциплину	2					[1,3, 4, 8, 13]	
РАЗДЕЛ 1.	**ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**							
Тема 2.	Основные понятия информационной безопасности и защиты информации	2					[3,4, 6, 8, 13]	
2.1	*Практическая работа №1.* Правовое обеспечение информационной безопасности		2				МУ	ПР*
Тема 3.	Анализ угроз информационной безопасности	2					[4, 6, 7, 12]	КТ*
3.1	*Практическая работа №2.* Анализ рисков информационной безопасности.		2				МУ	ПР*
РАЗДЕЛ 2.	**ПРАВОВОЕ ОБЕСПЕЧЕНИЕ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**							
Тема 4.	Правовое обеспечение защиты информации	2					[6,8,9,10, 11,12,14]	
Тема 5.	Виды компьютерных преступлений. Компьютерные вирусы	2					[4,5,7,11]	
5.1	*Практическая работа №3.* Выявление и фиксация следов противоправной деятельности на ПЭВМ.		2				МУ	ПР*
РАЗДЕЛ 3	**ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**							
Тема 6.	Государственное регулирование в области защиты информации	2					[6,8,9, 10,11]	
6.1	*Практическая работа №4.*		2				МУ	ПР*

Номер раздела темы	Название раздела, темы	Количество аудиторных часов					Литература	Формы контроля знаний
		лекции	практические занятия	семинарские занятия	лабораторные занятия	управляемой самостоятельной работы студента		
	Мероприятия по выявлению каналов утечки информации (специальные проверки)							
6.2	*Практическая работа №5.* Мероприятия по выявлению каналов утечки информации (специальные обследования)		2				МУ	ПР*
Тема 7.	Инженерно-техническая защита объектов от несанкционированного доступа	2						КТ*
7.1	*Практическая работа №6* Работа со звуком		2				МУ	ПР*
РАЗДЕЛ 4.	**ЭЛЕМЕНТЫ ТЕОРИИ СЛОЖНОСТИ. ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ**							
Тема 8.	Количество информации. Энтропия	2					[5,15,16]	КТ*
8.1	*Практическая работа №7.* Понятие информационной энтропии.		2				МУ	ПР*
РАЗДЕЛ 5.	**КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ**							
Тема 9.	Основные понятия криптографической защиты информации	2					[2,4,5,16]	
9.1	*Практическая работа №8.* Современные симметричные криптосистемы.		2				МУ	ПР*
9.1	*Практическая работа №9.* Современные асимметричные криптосистемы.		2				МУ	ПР*
Тема 10.	Функции хеширования и электронная цифровая подпись	2					[2,4,5,16, 17]	КТ*
10.1	*Практическая работа №10.* Функции хеширования и электронная цифровая подпись		2				МУ	ПР*
	Итого:	**20**	**20**					

* мероприятия текущего контроля

МУ – методические указания к выполнению практических работ

ПР – письменный отчет по практическим работам

КТ – компьютерный тест по лекционному материалу в рамках пройденной темы

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. - Москва: Горячая линия-Телеком, 2021. – 585 с.

2. Васильева, И.Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Юрайт, 2023. - 349 с. - Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника и практикума для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.

3. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие / В.Я. Ищейнов. – Москва Берлин: Директ-Медиа, 2020. - 271 с. – Текст электронный. – URL: https://biblioclub.ru/index.php?page=book&id=571485

4. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. - Санкт-Петербург: Лань, 2020 - 124 с.// ЭБС Лань. – Режим доступа: по подписке: URL: https://e.lanbook.com/book/133924

5. Раханов,К.Я. Обеспечение конфиденциальности информации в сети интернет: пособие / Министерство образования РБ, Полоцкий государственный университет. - Новополоцк: ПГУ, 2021. - 191 с.

6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Взамен: ГОСТ Р 50922-96; введ. 2008-02-01. – М.: Стандартинформ, 2007. – 12 с.

7. Бузов, Г.А. Выявление специальных технических средств несанкционированного получения информации. - Москва: Горячая линия-Телеком, 2021. - 203 с.

8. «Об информатизации»: Закон Республики Беларусь от 6 сентября 1995г. № 3850-XII // Ведомости Верховного Совета Республики Беларусь. Ноябрь 1995 г. № 33(179), ст. 428.

9. СТБ 34.101.1-2004 (ИСО/МЭК 15408.1-99) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

10. СТБ 34.101.2-2004 (ИСО/МЭК 15408.2-99) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

11. СТБ II ИСО/МЭК 17799-2000/2004 Информационные технологии и безопасность. Правила управления информационной безопасностью.

12. ТР 2013/027/BY – Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность».

Дополнительная:

13. Галатенко, В.А. Основы информационной безопасности: курс лекций. / В.А. Галатенко. – М.: Интернет-Университет Информационных Технологий, 2003. – 280 с.

14. Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие. / Ю.А. Родичев. – СПб.: Питер, 2008.

15. Семкин, С.И. Основы организационного обеспечения информационной безопасности объектов информатизации. / С.И. Семкин, Э.В. Беляков, С.В. Гребнев, В.И. Козачок. – М.: Гелиос АРВ, 2005. – 192с.

16. Богуш, Р.П. Основы защиты информации : учеб.-метод. комплекс для слушателей ИПК спец. 1-40 01 73 "Программное обеспечение информационных систем" / М-во образования РБ, Полоцкий гос. ун-т. - Новополоцк : ПГУ, 2009. - 95 с.

17. Безопасность электронного документооборота [Электронный ресурс]: учебное пособие / П. А. Тищенко, Ю. М. Казаков, Р. А. Филиппов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 54 с. – Режим доступа: по подписке: URL: https://biblioclub.ru/index.php?page=book&id=602225

ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ПРОГРАММ:

Используются пакеты: Matlab, Mathcad, PyCharm, Visual Code.

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическая работа №1 Правовое обеспечение информационной безопасности.

Практическая работа №2 Анализ рисков информационной безопасности.

Практическая работа №3 Выявление и фиксация следов противоправной деятельности на ПЭВМ.

Практическая работа №4. Мероприятия по выявлению каналов утечки информации (специальные проверки)

Практическая работа №5. Мероприятия по выявлению каналов утечки информации (специальные обследования)

Практическая работа №6. Работа со звуком

Практическая работа №7 Понятие информационной энтропии.

Практическая работа №8 Современные симметричные криптосистемы.

Практическая работа №9 Современные асимметричные криптосистемы.

Практическая работа №10 Функции хеширования и электронная цифровая подпись

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

1. Назовите основные проблемы информационной безопасности в современном мире.
2. Какие законы РБ в области ЗИ вы знаете? Назовите приоритетные направления в РБ в области защиты информации.
3. Укажите государственные органы и учреждения, занимающиеся вопросами защиты информации в РБ.
4. Назовите отличительные черты информационного общества. Дайте понятие информации.
5. Разделите понятия потребители и обладатели информации.
6. Перечислите основные компоненты безопасности. Что понимается под безопасностью?
7. Приведите основные элементы в структуре системы безопасности.
8. Перечислите аспекты информационной безопасности.
9. Укажете задачи, решение которых должна обеспечивает информационная безопасность.
10. Что включает в себя системная методология информационной безопасности?
11. Сформулируйте основные понятия в области защиты информации.
12. Приведите классификацию угроз. Приведите полную классификацию методов защиты информации.
13. Что относится к охраняемым сведениям? Приведите примеры демаскирующих признаков.
14. Расскажите, что вы знаете о содержании Закона РБ от 6 сентября 1995 г. № 3850-XII «Об информатизации»?
15. Расскажите, что вы знаете о содержании Закона РБ от 29 ноября 1994 г. № 3411-XII «О государственных секретах».
16. Расскажите, что вы знаете о содержании Закона РБ от 3 декабря 1997 г. № 102-З «Об органах государственной безопасности Республики Беларусь».
17. Приведите основное содержание Постановления Совета Министров РБ от 15 февраля 1999 г. № 237 «О служебной информации ограниченного распространения».
18. Приведите основное содержание Постановления Совета Министров РБ от 10 февраля 2000 г. № 186 «О некоторых мерах по защите информации в Республике Беларусь».
19. Что содержится в Указе Президента Республики Беларусь от 12 мая 2004 г. № 231 «Вопросы Государственного центра безопасности информации при Президенте Республики Беларусь»?
20. Что включает в себя правовая защита от компьютерных преступлений?

21. Перечислите виды компьютерных преступлений. Приведите примеры наиболее известных компьютерных преступлений, принесших значительный ущерб.
22. Какие существуют виды компьютерных преступлений? Что вам известно о мошенничестве в интернете.
23. Какие специальные программные средства используют мошенники в интернет?
24. Какими правилами следует руководствоваться, чтобы обезопасить себя от мошенничества в интернет?
25. Что вам известно о компьютерных вирусах и антивирусных программах? Приведите наиболее значимые исторические факты о компьютерных вирусах.
26. Дайте понятие вирус. Приведите пример классификации компьютерных вирусов.
27. Расскажите об особенностях алгоритмов работы наиболее распространенных вирусов, вредоносного программного обеспечения. Деструктивные возможности и пути проникновения вирусов. Какие существуют методы защиты от компьютерных вирусов?
28. Что означает Государственное регулирование в области защиты информации?
29. Сформулируйте основные положения государственной политики информационной безопасности РБ.
30. Дайте понятия «Система информационной безопасности РБ», «Государственная система защиты РБ».
31. Перечислите основные функции системы информационной безопасности. Какие проводятся в Республике мероприятия по защите информации?
32. Что вам известно о лицензировании деятельности юридических и физических лиц в области защиты информации.
33. Перечислите основные виды лицензируемой деятельности и основные требования к организациям, претендующим на получение лицензий на работы в области защиты информации.
34. Расскажите, как осуществляется сертификация и аттестация средств защиты информации.
35. Что включают в себя организационно-административные и организационно-технические методы защиты информации?
36. Расскажите о страховании как методе защиты информации.
37. Какие вам известны криптографические методы защиты информации?
38. Дайте основные понятия: криптология, криптография, криптоанализ.
39. Дайте понятия код, шифр и ключ: открытый и закрытый.
40. Приведите основную схему криптографии.
41. Дайте понятие электронного документа и электронной цифровой подписи

42. Придание юридического статуса электронным документам. Юридическая сила оригинала и копии электронного документа.
43. Какие существуют угрозы цифровой подписи. RSA как фундамент электронной цифровой подписи.
44. Приведите примеры уникальной и точной идентификации продуктов и банковских счетов.
45. Особенности использования стандартизированных кодов банков, супермаркетов и других крупных подсистем экономики – кредитные карты. Алгоритм Луна. Понятие и разновидности шрихкодов.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Управление информационной безопасностью» предполагает реализацию следующих видов самостоятельной работы студентов:

– подготовку к аудиторному выполнению практических работ (предварительное знакомство с методическими указаниями, программным обеспечением, вариантом индивидуального задания по работе);

– подготовку к защите практических работ (оформление отчета по индивидуальному варианту задания, защита результатов работы и демонстрации степени освоения навыков и умений по конкретной теме);

– решение индивидуальных задач при подготовке к практическим занятиям;

– изучение основной, дополнительной и научной литературы в процессе подготовки к анализу и решению проблемных задач, реализации элементов исследовательской деятельности;

– систематизация полученных знаний при подготовке к зачету.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации образовательного процесса, обеспечиваются:

– наличием и использованием в образовательном процессе платформы moodle.psu.by;

–наличием и полной доступностью электронных вариантов курса лекций и учебно-методического пособия по основным разделам дисциплины.

Содержание самостоятельной работы студентов (дневная форма получения высшего образования)

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Углубленное изучение отдельных тем для подготовки к контрольному тестированию	Тема 1. Литература [1,2,8,13]	2
	Тема 2. Литература [1,2,6,8,13]	2
	Тема 3. Литература [2,6,7,12]	3
	Тема 4. Литература [3,5,15]	3
	Тема 5. Литература [6,8,9,10,11,12,14]	3
	Тема 6. Литература [2,5,7,11]	3
	Тема 7. Литература [1,5,13]	3
	Тема 8. Литература [6,8,9,10,11]	3
	Тема 9. Литература [2,8,12,14]	3
	Тема 10. Литература [5,15,16]	3
Подготовка к защите отчетов по практическим работам	**Практическая работа №1** Методические указания	4
	Практическая работа №2 Методические указания	4
	Практическая работа №3 Методические указания	4
	Практическая работа №4 Методические указания	4
	Практическая работа №5 Методические указания	4
	Практическая работа №6 Методические указания	4
	Практическая работа №7 Методические указания	4
	Практическая работа №8 Методические указания	4
	Практическая работа №9 Методические указания	4
	Практическая работа №10 Методические указания	4
	ВСЕГО:	**68**

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Диагностика качества усвоения знаний проводится в форме текущего контроля и промежуточной аттестации.

Мероприятия текущего контроля проводятся в течение семестра и включают в себя следующие формы контроля:

– контрольное компьютерное тестирование;

– защита отчетов по практическим работам.

Практические занятия предполагают выполнение и защиту. При выполнении практических работ выдается индивидуальное задание. Отчет по практической работе представляется в электронном виде. Содержание отчета: название работы, вариант задания, анализ задания, ход выполнения работы, основные и промежуточные результаты, выводы по работе. Защита работ проводится индивидуально и оценивается в соответствии установленными правилами.

Результат *текущего контроля за семестр* оценивается отметкой в баллах по десятибалльной шкале и выводится, исходя из отметок, выставленных в ходе проведения мероприятий текущего контроля в течение семестра по следующей формуле:

$$\text{Т} = \frac{(\text{КТ}_1 + \ldots + \text{КТ}_4) + (\text{ПР}_1 + \ldots + \text{ПР}_{10})}{14}$$

где $\text{КТ}_1 + \ldots + \text{КТ}_n$ – отметки, выставленные по результатам контрольного тестирования;

$\text{ПР}_1 + \ldots + \text{ПР}_m$ – отметки, выставленные по результатам защит практических работ.

Для обучающего, пропустившего мероприятие текущего контроля по уважительной причине, кафедрой устанавливаются дополнительные сроки.

Обучающемуся, пропустившему мероприятие текущего контроля без уважительной причины, выставляется 1 (один) балл за данное мероприятие.

Результат текущего контроля может быть повышен:

- за участие обучающегося в научно-практических мероприятиях, учебно-исследовательской, научно-исследовательской работе студентов (конференциях, семинарах, олимпиадах, конкурсах, научных кружках и т.п.) по профилю учебной дисциплины (модуля) и может быть повышен до 10 баллов при достижении значимых результатов в этой работе;

- обучающийся в целях повышения отметки по любому мероприятию текущего контроля может воспользоваться правом на дополнительные образовательные услуги (платные консультации, платные дополнительные занятия). Количество и сроки пересдач с целью повышения отметки определяет кафедра.

Промежуточная аттестация проводится в форме зачета.

Заключение о *зачете* формируется по формуле:

$$З = k \cdot Т,$$

где k– весовой коэффициент текущего контроля;

Т – результат текущего контроля за семестр.

Весовой коэффициент k принимается равным 1.

Если полученная отметка $З < 4$ баллов, то проводится устный зачет отдельно по представленным в программе вопросам.

Перевод отметки по зачёту осуществляется по следующим правилам: отметка «зачтено» выставляется студентам, получившим от 4 до 10 баллов, отметка «не зачтено» выставляется студентам, получившим от 1 до 3 баллов.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Используемые технологии обучения и диагностики компетенций в преподавании учебной дисциплины «Управление информационной безопасностью» реализуют подход, основанный на максимально возможном использовании внутренней и учебной мотивации студента, проявляющейся в четком понимании им значимости всех видов выполняемых работ, как с точки зрения важности для профессиональной подготовки, так и с точки зрения оценивания. Подход предполагает использование элементов проблемного обучения и элементов исследовательской деятельности студентов в процессе аудиторной работы, а также при выполнении самостоятельных работ при постоянном рейтинговом контроле.

На лекционных занятиях по дисциплине «Управление информационной безопасностью» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Изучение учебной дисциплины осуществляется на лекционных и практических занятиях. На лекционных занятиях студенты овладевают системой теоретических знаний в области защиты информации. В ходе лекционного изложения теоретических сведений используются традиционные словесные приемы и методы, которые активизируются постановкой проблемных вопросов и заданий, организацией учебных дискуссий в опоре на имеющуюся начальную подготовку студентов и их политехнический кругозор, использованием интерактивных методов обучения.

На практических занятиях развиваются и формируются необходимые практические умения и навыки по оценке защищенности компьютерных систем и технических каналов утечки. Во время проведения практических работ особое внимание уделяется формированию у студентов умения планировать работу, определять эффективную последовательность ее выполнения.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу
Дипломное проектирование	кафедра мировой литературы и иностранных языков	нет	

Зав. кафедрой мировой литературы
и иностранных языков, к.ф.н. _____ Е.В. Лушневская