Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования
«Полоцкий государственный
университет имени
Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«13» 12 2025 г.
Регистрационный №УД-49225/уч.

СИСТЕМЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ

Учебная программа учреждения образования
по учебной дисциплине для специальности
6-05-0533-12 «Кибербезопасность»

2025 г.

Учебная программа составлена на основе образовательного стандарта по специальности высшего образования ОСВО 6-05-0533-12-2023 и учебного плана специальности 6-05-0533-12 «Кибербезопасность». Регистрационный №14-23/уч. ФКНЭ от 04.04.2023 г. для дневной формы получения высшего образования.

СОСТАВИТЕЛЬ:

Ирина Брониславовна Бураченок, к.т.н., доцент, доцент кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 11 от « 21 » 11 2025 г.).

Научно-методическим советом учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 3 от « 15 » 12 2025 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Целью кибербезопасности является обеспечение трех наиболее важных принципов: конфиденциальности, целостности и доступности информации. Информация и данные должны быть постоянно легко доступны и в то же время надежно защищены от неправомерного использования. Искажение или фальсификация, уничтожение или разглашение определенной части информации, также, как и нарушение процессов её обработки и передачи, наносят серьезный урон субъектам информационного взаимодействия. В сложной геополитической ситуации актуальны случаи цифровых атак, которые могут навредить и репутации компании. Защита особенно важна для таких типов информации, как служебная, коммерческая, медицинская, а также для персональных данных. Исходя из этого, учебная дисциплина «Системы обеспечения комплексной безопасности» ориентирована на обучение студентов базовым знаниям, умениям и навыкам в области обеспечения комплексной информационной безопасности и защиты информации и ориентирована на подготовку специалиста, умеющего создавать защищенные информационные системы и исследовать защищенность компьютерно-коммуникационных систем.

Изучаемые темы представляются на основе современной нормативной регулятивной базы и национального законодательства.

Целью изучения дисциплины «Системы обеспечения комплексной безопасности» является формирование у студентов системного взгляда на проблему защиты информации в разрабатываемых, эксплуатируемых или сопровождаемых информационных системах и формирование у них знаний и навыков, необходимых для понимания и применения различных методов и методик обеспечения безопасности в широком диапазоне систем и организаций, а также общих подходов и инструментов для достижения одной практической цели: защиты от любых возможных и обнаруженных угроз, таких как несанкционированная утечка, замена или потеря данных.

Изучение данной дисциплины является необходимым этапом в профессиональном развитии «специалиста по кибербезопасности».

Задачи изучения дисциплины «Системы обеспечения комплексной безопасности». При изучении данной дисциплины требуется разрешить основные задачи:

– сформировать у студентов понимание базовых понятий, связанных с процессом обеспечения комплексной безопасности;

– показать основные угрозы безопасности объектов информатизации;

– сформировать системное понимание обеспечения комплексной безопасности объекта информатизации.

При изучении дисциплины «Системы обеспечения комплексной безопасности» у студентов специальности 6-05-0533-12 «Кибербезопасность» должен сформироваться набор компетенций, соответствующих присваиваемой по завершению высшего образования квалификации «специалист по кибербезопасности», обеспечивающих выпускникам по указанной специальности успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности:

специализированные компетенции

– Использовать основные понятия и нормативные правовые акты информационной безопасности для описания и классификации теоретических, правовых, организационных и инженерно-технических методов обеспечения конфиденциальности, целостности и доступности информации.

Сформированные компетенции являются базовыми при изучении всех последующих дисциплин, связанных с программированием, а также фундаментальной основой для дальнейшей профессиональной деятельности специалиста в области кибербезопасности.

В результате изучения дисциплины «Системы обеспечения комплексной безопасности» обучаемый должен

знать:

– основные принципы и концепции комплексной системы безопасности;

– технологии обеспечения комплексной безопасности критически важных объектов информатизации с использованием внутренних ресурсов, а также имеющимися на рынке готовыми решениями в соответствии с требованиями Оперативно-аналитического центра при Президенте Республики Беларусь (ОАЦ);

– современные методы и технологии, используемые в комплексных системах безопасности, включая средства инженерной защиты: системы видеонаблюдения, системы управления и контроля доступа (СКУД), системы охранной и пожарной безопасности и т.д.

– известные DLP (Data Loss Prevention) системы для контроля каналов / потоков передачи, классификация конфиденциальной информации, выявление и предотвращение утечек критичных данных;

– известные IDS (Intrusion Detection System) / IPS (Intrusion Prevention System) системы для обнаружения / предотвращения кибервторжений;

– известные SIEM (Security Information and Event Management) системы для управления информацией и событиями безопасности;

– известные IDM (Identity management) программные комплексы корпоративного уровня объединяющие методы, технологии и практики для управления учетными данными пользователей, системами контроля, включая СКУД,

уметь:

– разрабатывать и внедрять политику и процедуры обеспечения комплексной безопасности на предприятии с целью предотвращения рисков утечки информации и потери данных;

– проектировать и разрабатывать комплексные системы безопасности;

– анализировать и оценивать угрозы и риски в области безопасности, а также разрабатывать меры по их предотвращению и устранению;

– осуществлять мониторинг и аудит эффективности мер безопасности, для своевременного обнаружения и устранения слабых мест;

– обнаруживать инциденты в режиме реального времени;

– реагировать на обнаруженные инциденты безопасности и проводить расследование инцидентов и осуществлять сбор доказательной базы;

– выбирать актуальные инструменты и технические средства защиты информации, минимизирующие угрозы несанкционированного доступа к данным;

– работать с программным обеспечением и аппаратным обеспечением, применяемыми в комплексных системах безопасности,

владеть:

– навыками работы с информационными источниками и нормативными документами по вопросам обеспечения комплексной безопасности;

– методами и технологиями обеспечения комплексной безопасности.

Связи с другими учебными дисциплинами.

Основой для изучения учебной дисциплины «Системы обеспечения комплексной безопасности» по специальности 6-05-0533-12 «Кибербезопасность» является учебный предмет «Информатика», изучаемый при получении общего базового и общего среднего образования, а также необходимы знания, полученные при изучении базовых учебных дисциплин «Программирование на C++», «Разработка кросс-платформенных приложений», «Программирование на Python», «Технологии программирования», «Машинно-ориентированное программирование», «Архитектура компьютеров», «Алгоритмы и структуры данных», «Базы данных», «Операционные системы», «Компьютерные сети», «Защита информации в операционных системах и компьютерных сетях», «Защита от вредоносного программного обеспечения».

Знания, полученные при изучении дисциплины «Системы обеспечения комплексной безопасности», являются основой для дипломного проектирования. Изучение учебной дисциплины позволяет дать студентам знания, необходимые в дальнейшем для успешной работы по специальности.

Форма получения высшего образования – дневная.

В соответствии с учебным планом по специальности 6-05-0533-12 «Кибербезопасность» на изучение учебной дисциплины отводится:

Курс (курсы)	3
Семестр	6
Всего часов по дисциплине	108
Всего аудиторных часов по дисциплине	52
В том числе:	
Лекции, часов	34
Лабораторные занятия, часов	18
Самостоятельная работа, часов	56
Форма промежуточной аттестации	зачет
Трудоёмкость дисциплины, з.е.	3

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

ВВЕДЕНИЕ В ДИСЦИПЛИНУ

Цели и задачи изучения дисциплины. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале.

Раздел 1. МЕТОДОЛОГИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Тема 1.1. Сущность и задачи комплексной защиты информации на предприятии.

Понятийный аппарат в области обеспечения информационной безопасности на предприятии. Цели, задачи и принципы построения комплексной системы защиты информации (КСЗИ). Управление безопасностью предприятия. Международные стандарты. Цели и задачи защиты информации в автоматизированных системах (АС). Современное понимание методологии защиты информации: особенности национального технического регулирования, современные требования к средствам обеспечения безопасности.

Тема 1.2. Принципы организации и этапы разработки комплексной системы защиты информации

Принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ. Методологические основы организации комплексной системы защиты информации. Разработка политики безопасности и регламента безопасности предприятия. Основные положения теории сложных систем. Система управления информационной безопасностью предприятия. Требования, предъявляемые к комплексной системе защиты информации. Этапы разработки комплексной системы защиты информации.

Тема 1.3. Факторы, влияющие на организацию комплексной системы защиты информации.

Влияние формы собственности на особенности защиты информации ограниченного доступа. Характер основной деятельности предприятия. Структура и территориальное расположение предприятия. Режим функционирования предприятия. Состав, объекты и степень конфиденциальности защищаемой информации. Конструктивные особенности предприятия. Степень автоматизации основных процедур обработки защищаемой информации.

Раздел 2. ПОСТРОЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 2.1. Определение и нормативное закрепление состава защищаемой информации

Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. Нормативно-правовые аспекты определения состава защищаемой информации. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия. Методика определения состава защищаемой информации.

Тема 2.2. Определение объектов защиты

Значение носителей защищаемой информации как объектов защиты. Методика выявления состава носителей защищаемой информации. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.

Тема 2.3. Определение компонентов комплексной системы защиты информации

Факторы, влияющие на выбор компонентов КСЗИ. Объекты защиты как основной фактор, определяющий состав компонентов КСЗИ. Основные требования, предъявляемые к выбору методов и средств защиты, зависимость. их от структуры предприятия, защищаемых элементов объектов, условий функционирования КСЗИ. Проектирование системы защиты информации для существующей АС.

Тема 2.4. Определение условий функционирования комплексной системы защиты информации

Содержание концепции построения комплексной системы защиты информации. Объекты защиты. Цели и задачи обеспечения безопасности информации. Основные угрозы безопасности информации АС организации. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию. Определение потенциальных каналов и методов несанкционированного доступа (НСД) к информации. Определение возможностей НСД к защищаемой информации.

Тема 2.5. Основные принципы построения комплексной системы защиты информации

Основные принципы построения комплексной системы защиты информации. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.

Тема 2.6. Разработка модели комплексной системы защиты информации

Общая характеристика задач моделирования комплексной системы защиты информации. Формальные модели безопасности и их анализ: классификация формальных моделей безопасности; модели обеспечения конфиденциальности; модели обеспечения целостности; субъектно-ориентированная модель. Технологическое и организационное построение КСЗИ.

РАЗДЕЛ 3. ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 3.1. Кадровое обеспечение функционирования комплексной системы защиты информации

Специфика персонала предприятия как объекта защиты. Распределение функций по защите информации: функции руководства предприятия; функции службы защиты информации; функции специальных комиссий; обязанности пользователей защищаемой информации. Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа. Подбор и обучение персонала.

Тема 3.2. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации.

Состав и значение материально-технического обеспечения функционирования комплексной системы защиты информации. Перечень вопросов ЗИ, требующих документационного закрепления.

Раздел 4. УПРАВЛЕНИЕ КОМПЛЕКСНОЙ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 4.1. Назначение, структура и содержание управления комплексной системы защиты информации

Понятие, сущность и цели управления комплексной системы защиты информации. Принципы управления комплексной системы защиты информации. Структура процессов управления. Основные процессы, функции и задачи управления комплексной системы защиты информации.

Тема 4.2. Принципы и методы планирования функционирования комплексной системы защиты информации.

Понятие и задачи планирования функционирования комплексной системы защиты информации. Способы и стадии планирования. Факторы, влияющие на выбор способов планирования. Основы подготовки и принятия решений при планировании. Методы сбора, обработки и изучения информации, необходимой для планирования. Организация выполнения планов. ГОСТ 34.201-89.

Тема 4.3. Сущность и содержание контроля функционирования комплексной системы защиты информации

Виды контроля функционирования комплексной системы защиты информации. Цель проведения контрольных мероприятий в комплексной системы защиты информации. Анализ и использование результатов проведения контрольных мероприятий. ГОСТ 34.601-90.

Тема 4.4. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций

Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях ЧС. Факторы, влияющие на принятие решений в условиях ЧС. Подготовка мероприятий на случай возникновения ЧС.

Раздел 5. ОЦЕНКА ЭФФЕКТИВНОСТИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 5.1. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации.

Вероятностный подход. Оценочный подход. Требования РД СВТ и РД АС. Задание требований безопасности информации и оценка соответствия им согласно ГОСТ 15408-2002. Экспериментальный подход. ГОСТ 34.603-92.

Тема 5.2. Состав методов и моделей оценки эффективности комплексной системы защиты информации.

Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса. Экономический подход к оценке эффективности комплексной системы защиты информации.

Учебно-методическая карта учебной дисциплины «Системы обеспечения комплексной безопасности»
Дневная форма получения высшего образования

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		лекции	Лабораторные занятия	Практические занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
	Введение в дисциплину Цели и задачи изучения дисциплины. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале.					Осн. лит.: [1]. Доп. лит.: [1].	
	Раздел 1 Методология комплексной защиты информации на предприятии	**6**		**2**			
1	**Лекция № 1** *Тема 1.1. Сущность и задачи комплексной защиты информации на предприятии.* Понятийный аппарат в области обеспечения информационной безопасности на предприятии. Цели, задачи и принципы построения комплексной системы защиты информации (КСЗИ). Управление безопасностью предприятия. Международные стандарты. Цели и задачи защиты информации в автоматизированных системах (АС). Современное понимание методологии защиты информации: особенности национального технического регулирования, современные требования к средствам обеспечения безопасности.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [5], [7].	Блиц-опрос
2	**Лекция № 2** *Тема 1.2. Принципы организации и этапы разработки комплексной системы защиты информации.*	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [5], [7].	Блиц-опрос

1	2	3	4	5	6	7	8
	Принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ. Методологические основы организации комплексной системы защиты информации. Разработка политики безопасности и регламента безопасности предприятия. Основные положения теории сложных систем. Система управления информационной безопасностью предприятия. Требования, предъявляемые к комплексной системе защиты информации. Этапы разработки комплексной системы защиты информации.						
3	**Лабораторная работа №1** Изучение алгоритмов и условия сжатия изображения с видеокамеры.			2		Методические указания	*Защита отчета по лабораторной работе № 1
4	**Лекция № 3** *Тема 1.3. Факторы, влияющие на организацию комплексной системы защиты информации.* Влияние формы собственности на особенности защиты информации ограниченного доступа. Характер основной деятельности предприятия. Структура и территориальное расположение предприятия. Режим функционирования предприятия. Состав, объекты и степень конфиденциальности защищаемой информации. Конструктивные особенности предприятия. Степень автоматизации основных процедур обработки защищаемой информации.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	*Контрольное тестирование №1
	Раздел 2 Построение комплексной системы защиты информации	**12**		**6**			
5	**Лекция № 4** *Тема 2.1. Определение и нормативное закрепление состава защищаемой информации.* Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. Нормативно-правовые аспекты определения состава защищаемой информации. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия. Методика определения состава защищаемой информации.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	Блиц-опрос

1	2	3	4	5	6	7	8
6	**Лабораторная работа №2** Изучение конструкции, характеристик и принципа работы видеокамер.			2		Методические указания	*Защита отчета по лабораторной работе № 2
7	**Лекция № 5** *Тема 2.2. Определение объектов защиты.* Значение носителей защищаемой информации как объектов защиты. Методика выявления состава носителей защищаемой информации. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [4], [6], [7].	Блиц-опрос
8	**Лекция № 6** *Тема 2.3. Определение компонентов комплексной системы защиты информации.* Факторы, влияющие на выбор компонентов КСЗИ. Объекты защиты как основной фактор, определяющий состав компонентов КСЗИ. Основные требования, предъявляемые к выбору методов и средств защиты, зависимость. их от структуры предприятия, защищаемых элементов объектов, условий функционирования КСЗИ. Проектирование системы защиты информации для существующей АС.	2				Осн. лит.: [1], [2], [3], [4]. Доп. лит.: [1], [3], [6], [7].	Блиц-опрос
9	**Лабораторная работа №3** Проектирование систем видеонаблюдения.			2		Методические указания	*Защита отчета по лабораторной работе № 3
10	**Лекция № 7** *Тема 2.4. Определение условий функционирования комплексной системы защиты информации.* Содержание концепции построения комплексной системы защиты информации. Объекты защиты. Цели и задачи обеспечения безопасности информации. Основные угрозы безопасности информации АС организации. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию. Определение потенциальных каналов и методов (НСД). Определение возможностей НСД к защищаемой информации.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	***Контрольная работа №1**

1	2	3	4	5	6	7	8
11	**Лекция № 8** *Тема 2.5. Основные принципы построения комплексной системы защиты информации.* Основные принципы построения комплексной системы защиты информации. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	***Контрольная работа №1**
12	**Лабораторная работа №4** Проектировании систем автоматического распознования лиц в видеонаблюдении.			2		Методические указания	*Защита отчета по лабораторной работе № 4
13	**Лекция №9** *Тема 2.6. Разработка модели комплексной системы защиты информации.* Общая характеристика задач моделирования комплексной системы защиты информации. Формальные модели безопасности и их анализ: классификация формальных моделей безопасности; модели обеспечения конфиденциальности; модели обеспечения целостности; субъектно-ориентированная модель. Технологическое и организационное построение КСЗИ.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	*Контрольное тестирование №2
	Раздел 3 Обеспечение комплексной системы защиты информации	**4**		**2**			
14	**Лекция №10** *Тема 3.1. Кадровое обеспечение функционирования комплексной системы защиты информации.* Специфика персонала предприятия как объекта защиты. Распределение функций по защите информации: функции руководства предприятия; функции службы защиты информации; функции специальных комиссий; обязанности пользователей защищаемой информации. Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа. Подбор и обучение персонала.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	Блиц-опрос
15	**Лабораторная работа №5** Проектирование системы контроля и управления доступом.			2		Методические указания	*Защита отчета по лабораторной работе № 5

1	2	3	4	5	6	7	8
16	**Лекция №11** *Тема 3.2. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации.* Состав и значение материально-технического обеспечения функционирования комплексной системы защиты информации. Перечень вопросов ЗИ, требующих документационного закрепления.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	*Контрольное тестирование №3
	Раздел 4 Управление комплексной системой защиты информации	**6**		**4**			
17	**Лекция №12** *Тема 4.1 Назначение, структура и содержание управления комплексной системы защиты информации.* Понятие, сущность и цели управления комплексной системы защиты информации. Принципы управления комплексной системы защиты информации. Структура процессов управления. Основные процессы, функции и задачи управления комплексной системы защиты информации.	2				Осн. лит.: [1], [4]. Доп. лит.: [2], [3], [7].	Блиц-опрос
18	**Лабораторная работа №6** Изучение средств пожарной сигнализации.			2		Методические указания	*Защита отчета по лабораторной работе № 6
19	**Лекция №13** *Тема 4.2. Принципы и методы планирования функционирования комплексной системы защиты информации.* Понятие и задачи планирования функционирования комплексной системы защиты информации. Способы и стадии планирования. Факторы, влияющие на выбор способов планирования. Основы подготовки и принятия решений при планировании. Методы сбора, обработки и изучения информации, необходимой для планирования. Организация выполнения планов. ГОСТ 34.201-89.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	Блиц-опрос
20	**Лекция №14** *Тема 4.3. Сущность и содержание контроля функционирования комплексной системы защиты информации.* Виды контроля функционирования комплексной системы защиты информации. Цель проведения контрольных мероприятий в комплексной системы защиты информации. Анализ и использование результатов проведения контрольных мероприятий. ГОСТ 34.601-90.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	Блиц-опрос

1	2	3	4	5	6	7	8
21	**Лабораторная работа №7** Изучение системы для управления информацией и событиями безопасности SIEM (Security Information and Event Management). Моделирование процесса реагирования на киберинциденты с использованием WAZUH.			2		Методические указания	*Защита отчета по лабораторной работе № 7
22	**Лекция №15** *Тема 4.4. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций.* Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях ЧС. Факторы, влияющие на принятие решений в условиях ЧС. Подготовка мероприятий на случай возникновения ЧС.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	***Контрольная работа №2**
	Раздел 5 Оценка эффективности комплексной системы защиты информации	**4**		**4**			
23	**Лекция №16** *Тема 5.1. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации.* Вероятностный подход. Оценочный подход. Требования РД СВТ и РД АС. Задание требований безопасности информации и оценка соответствия им согласно ГОСТ 15408-2002. Экспериментальный подход. ГОСТ 34.603-92.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	Блиц-опрос
24	**Лекция №17** *Тема 5.2. Состав методов и моделей оценки эффективности комплексной системы защиты информации.* Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса. Экономический подход к оценке эффективности комплексной системы защиты информации.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	*Контрольное тестирование №4
25	**Лабораторная работа №8** Моделирование процесса реагирования на киберинциденты на примере работы с продуктами компании UserGate.			2		Методические указания	*Защита отчета по лабораторной работе № 8

1	2	3	4	5	6	7	8
26	**Лабораторная работа №9** Моделирование процесса реагиования на киберинциденты на примере работы с продуктами компании UserGate.			2		Методические указания	*Защита отчета по лабораторной работе № 9
	Всего (52 часов)	**34**		**18**			

*** МЕРОПРИЯТИЯ ТЕКУЩЕГО КОНТРОЛЯ**

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург : Лань, 2025. – 400 с. – ISBN 978-5-507-52839-4. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/460715 (дата обращения: 16.01.2026). – Режим доступа: для авториз. пользователей.

2. Головатая, Е.А. Нейросетевые технологии в обработке и защите данных : учебное пособие / Е. А. Головатая, А. В. Курочкин ; Белорусский государственный университет. – Минск : БГУ, 2021. – 150 с. – Допущено Министерством образования Республики Беларусь в качестве учебного пособия для студентов учреждений высшего образования по направлению специальности «Компьютерная безопасность (радиофизические методы и программно-технические средства)».

3. Интеллектуальные технологии информационной безопасности / О. И. Шелухин, Д. П. Зегжда, Д. И. Раковский [и др.]. – Москва : Горячая линия – Телеком, 2023. – 384 с.

4. Тумбинская М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник для вузов / М. В. Тумбинская, М. В. Петровский. – 3-е изд., стер. – Санкт-Петербург : Лань, 2025. – 344 с. : ил. – Текст : непосредственный.

Дополнительная:

1. Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации : учебное пособие / С. И. Козьминых ; Финансовый университет при Правительстве Российской Федерации. – Москва : Юнити-Дана, 2020. – 544 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=615695 (дата обращения: 16.01.2026). – Библиогр. в кн. – ISBN 978-5-238-03200-9. – Текст : электронный.

2. Мандрица И. В. Управление проектами по информационной безопасности и экономика защиты информации : учебник для вузов / И. В. Мандрица, В. И. Петренко, О. В. Мандрица. – Санкт- Петербург : Лань, 2023. – Часть 1. – 124 с. : ил. – Текст : непосредственный.

3. Петров, В. В. Комплексные системы безопасности современного города : учебное пособие / В. В. Петров, В. В. Коробкин, А. Б. Сивенко ; Южный федеральный университет, Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2017. – 158 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499967 (дата обращения: 16.01.2026). – Библиогр.: с. 136-144. – ISBN 978-5-9275-2587-4. – Текст : электронный.

4. Печищев, И.М. Информационная безопасность: как защитить себя и свои аккаунты. Онлайн курс доступа: https://stepik.org/course/68856/promo бесплатно). [Электронный ресурс] – URL: (дата обращения: 18.12.2024).

5. Системы защиты информации в ведущих зарубежных странах : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, М. В. Рудановский, Г. В. Кондрашин ; науч. ред. В. И. Аверченков. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 224 с. : ил., схем. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93351 (дата обращения: 16.01.2026). – Библиогр.: с. 192-193. – ISBN 978-5-9765-1274-0. – Текст : электронный.

6. Талипов, Н. Г. Интеллектуальные системы обеспечения информационной безопасности : учебное пособие / Н. Г. Талипов, А. С. Катасёв, Д. В. Катасёва. – Казань :

Гуркова Е.В.

КНИТУ-КАИ, 2022. – 156 с. – ISBN 978-5-7579-2596-7. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/366533 (дата обращения: 16.01.2026). – Режим доступа: для авториз. пользователей.

7. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. – Москва ; Вологда : Инфра-Инженерия, 2024. – 144 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=725640 (дата обращения: 16.01.2026). – Библиогр.: с. 102-104. – ISBN 978-5-9729-1610-8. – Текст : электронный.

8. Уорр, К. Надежность нейронных сетей / К. Уорр. – Санкт-Петербург : Питер, 2021. – 272 с.. – ISBN 978-5-4461-1676-8.

Нормативная литература:

1. ТР 2013/027/BY, BY. Информационные технологии. Средства защиты информации. Информационная безопасность : технический регламент Республики Беларусь : утв. Советом Министров Респ. Беларусь 15.05.2013 № 375 (в ред. постановления Совета Министров Респ. Беларусь 12.03.2020 № 145) : введ. 01.01.2014. – Минск, 2020. – II, 6 с.

2. Уголовный Кодекс Республики Беларусь, опубликованный в официальном периодическом печатном издании «Национальный реестр правовых актов Республики Беларусь», 1999 г., №76, 2/50, с изменениями, внесенными Законом Республики Беларусь №112-З от 26.05.2021 г. По состоянию на 9.09.2021 г.

3. Постановление Совета Министров Республики Беларусь. «О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну» №783 от 12.08.2014 г. – Режим доступа: https://pravo.by/document/?guid=3871&p0=C21400783 – Национальный правовой Интернет-портал Республики Беларусь.

4. Закон Республики Беларусь «Об органах государственной безопасности Республики Беларусь» № 390 от 10.07.2012 г. – Режим доступа: https://pravo.by/document/?guid=3871&p0=H11200390 – Национальный правовой Интернет-портал Республики Беларусь.

5. Закон Республики Беларусь «Об информации, информатизации и защите информации» №455-З от 10.11.2008 г. – Режим доступа: https://pravo.by/document/?guid=3871&p0=h10800455 – Национальный правовой Интернет-портал Республики Беларусь.

6. Закон Республики Беларусь «О государственных секретах» №170-З от 19.07.2010. [Электрон, ресурс]. – Режим доступа: http://www.minfin.gov.by/upload/gosznak/acts/zakon_190710_170z.pdf. – Дата доступа: 19.03.2023.

7. Закон Республики Беларусь «О коммерческой тайне» № 16-З от 05.01.2013 г. – Режим доступа: https://pravo.by/document/?guid=3871&p0=H11300016 – Национальный правовой Интернет-портал Республики Беларусь.

8. Закон Республики Беларусь «О защите персональных данных» №99-З от 07.05.2021 г. – Режим доступа: https://pravo.by/document/?guid=3871&p0=H12100099 – Национальный правовой Интернет-портал Республики Беларусь.

9. Указ Президента Республики Беларусь «О биометрических документах» №107 от 16.03.2021 г. – Режим доступа: https://pravo.by/document/?guid=3871&p0=P32100107 – Национальный правовой Интернет-портал Республики Беларусь

10. Указ Президента Республики Беларусь «О мерах по совершенствованию защиты персональных данных» №422 от 28.10.2021 г. – Режим доступа: https://president.gov.by/ru/documents/ukaz-no-422-ot-28-oktyabrya-2021-g – Пресс-служба Президента Республики Беларусь.

11. Указ Президента Республики Беларусь «О совершенствовании государственного регулирования в области защиты информации» №440 от 9.12.2019 г. – Режим доступа: https://president.gov.by/ru/documents/ukaz-449-ot-9-dekabrja-2019-g-22569 – Пресс-служба Президента Республики Беларусь.

12. Указ Президента Республики Беларусь «О кибербезопасности» №40 от 14.02.2023 г. – Режим доступа: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g – Пресс-служба Президента Республики Беларусь.

13. Указ Президента Республики Беларусь «О цифровом развитии» №381 от 29.11.2023 г. – Режим доступа: https://president.gov.by/ru/documents/ukaz-no-381-ot-29-noyabrya-2023-g – Пресс-служба Президента Республики Беларусь.

14. Концепция национальной безопасности Республики Беларусь, утв. решением Всебелорусского народного собрания №5 от 25.04.2024 г. – Режим доступа: https://pravo.by/document/?guid=3871&p0=P924v0005 – Национальный правовой Интернет-портал Республики Беларусь.

15. ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

16. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

17. ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

18. ГОСТ/ИСО МЭК 15408-2002 «Общие критерии оценки безопасности информационных технологий».

19. СТБ 34.101.30-2017, BY. Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация. – Взамен СТБ 34.101.30-2007; введ. 01.10.17. – Минск, 2017. – II, 6 с.

20. СТБ 34.101.72-2018, BY. Информационные технологии. Методы и средства безопасности. Технические средства обработки информации. Классификация угроз безопасности, связанных с наличием закладных устройств и недекларированных функций. – Взамен СТБ П 34.101.72-2015; введ. 01.08.18. – Минск, 2018. – II, 10 с.

21. СТБ 34.101.74-2017, BY. Информационные технологии. Система сбора и обработки данных событий информационной безопасности. Общие требования. — Введ. 01.10.17. – Минск, 2017. – II, 6 с. – Введен впервые.

22. СТБ 1250-2000. Охрана объектов и физических лиц. Термины и определения. - Введ. 2011-04-01. - Минск : Госстандарт Респ. Беларусь, 2001.

23. ГОСТ 26342-84. Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры. – Введ. 1986-01-01.

24. СТБ 2659-2024. «Умный город». Структура «умных городов» (введен в действие с 1 февраля 2025 г.)

25. СТБ ISO/IEC 27005-2024. Информационная безопасность, кибербезопасность и защита конфиденциальности.

Электронные ресурсы:

1. Научно-исследовательский институт технической защиты информации. [Электрон, ресурс]. – Режим доступа: http://www.niitzi.by. – Дата доступа: 20.09.2025.

2. Национальный правовой портал Республики Беларусь. [Электрон, ресурс]. – Режим доступа: https://www.pravo.by. – Дата доступа: 120.09.2025.

3. Оперативно-аналитический центр при Президенте Республики Беларусь [Электрон, ресурс]. – Режим доступа: https://www.oac.gov.by. – Дата доступа: 20.09.2025.

4. Министерство связи и информатизации Республики Беларусь. [Электрон, ресурс]. – Режим доступа: https://www.mpt.gov.by. – Дата доступа: 20.09.2025.

ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Лабораторная работа №1 Изучение алгоритмов и условия сжатия изображения с видеокамеры.

Лабораторная работа №2 Изучение конструкции, характеристик и принципа работы видеокамер.

Лабораторная работа №3 Проектирование систем видеонаблюдения.

Лабораторная работа №4 Проектировании систем автоматического распознования лиц в видеонаблюдении.

Лабораторная работа №5 Проектирование системы контроля и управления доступом.

Лабораторная работа №6 Изучение средств охранно-пожарной сигнализации.

Лабораторная работа №7 Изучение системы для управления информацией и событиями безопасности SIEM (Security Information and Event Management). Моделирование процесса реагиования на киберинциденты с использованием WAZUH.

Лабораторная работа №8 Моделирование процесса реагиования на киберинциденты на примере работы с продуктами компании UserGate.

Лабораторная работа №9 Моделирование процесса реагиования на киберинциденты на примере работы с продуктами компании UserGate.

ПЕРЕЧЕНЬ ТЕМ РЕФЕРАТОВ

1. Особенности разработки комплексной системы защиты информации коммерческой организации.
2. Разработка рекомендаций по использованию средств защиты от DDOS-атак в корпоративных сетях.
3. Исследование безопасности контактных и бесконтактных смарт-карт.
4. Разработка рекомендаций по повышению уровня информационной безопасности госбюджетной организации.
5. Совершенствование системы защиты информации производственного предприятия
6. Анализ возможностей обеспечения безопасности кроссплатформенных мобильных приложений.
7. Применение алгоритмов машинного обучения к задаче выявления мошенничества при пользовании банковскими услугами.
8. Системы распознавания бесхозных предметов, несущих угрозу, с использованием нейронных сетей.
9. Анализ развития и возможности использования сетей с нулевым доверием.
10. Анализ возможностей кибератак на нейросети в системах машинного зрения.
11. Исследование возможностей шлюза безопасности UserGate для обеспечения защиты информации, циркулирующей в корпоративной сети предприятия.
12. Использование технологии фаззинга для повышения безопасности информации, содержащейся в приложениях.
13. Анализ законодательства в области безопасности Интернета вещей.
14. Анализ уязвимостей в социальных сетях.
15. Организация защиты информационной системы малого предприятия.
16. Алгоритм определения параметров угроз информационной безопасности автоматизированных систем.
17. Комплекс защитных мер по обеспечению информационной безопасности баз данных.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

Введение в дисциплину

1. Цели и задачи изучения дисциплины.

2. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале.

Лекция №1

3. В чем состоит сущность комплексной защиты информации на предприятии?

4. Какова основная цель обеспечения информационной безопасности на предприятии?

5. Перечислите основные задачи комплексной защиты информации на предприятии?

6. Перечислите основные принципы построения комплексной системы защиты информации (КСЗИ).

7. Укажите известные вам международные стандарты безопасности.

8. Как организована защита информации в автоматизированных системах (АС)?

9. Современное понимание методологии защиты информации: особенности национального технического регулирования, современные требования к средствам обеспечения безопасности.

10. Укажите перечень владельцев критически важных объектов информатизации и вошедших в него юрлиц, а также поставщиков услуг хостинга официальных интернет-сайтов и электронной почты, которые после вступления в силу Указа Президента Республики Беларусь «О кибербезопасности» №40 от 14.02.2023 г создали свои внутренние центры кибербезопасности. Приведите перечень аттестованных центров кибербезопасности в Республике Беларусь.

Лекция №2

11. Перечислите принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ.

12. Методологические основы организации комплексной системы защиты информации.

13. Что понимают под политикой безопасности и регламентом безопасности предприятия?

14. Приведите основные положения теории сложных систем.

15. Что понимают под системой управления информационной безопасностью предприятия.

16. Какие требования, предъявляюте к комплексной системе защиты информации.

17. Перечислите этапы разработки комплексной системы защиты информации.

Лекция №3

18. Расскажите о влиянии формы собственности на особенности защиты информации ограниченного доступа.

19. Что понимают под понятием характер основной деятельности предприятия.

20. Как влияют структура и территориальное расположение предприятия на построение комплексной системы безопасности?

21. Что такое режим функционирования предприятия?

22. Состав, объекты и степень конфиденциальности защищаемой информации.

23. Автоматизация основных процедур обработки защищаемой информации.

Лекция №4

24. Какое значение имеют носители защищаемой информации?

25. Перечислите факторы, определяющие состав носителей информации.

26. Какие существуют нормативно-правовые аспекты определения состава защищаемой информации.

27. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия.

28. Опишите методику определения состава защищаемой информации.

Лекция №5

29. Какое имеют значение носители защищаемой информации как объектов защиты?

30. Приведите методику выявления состава носителей защищаемой информации.

31. Перечислите факторы, определяющие необходимость защиты периметра и здания предприятия.

32. Какие имеются особенности помещений как объектов защиты для работы по защите информации?

33. Приведите состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.

Лекция №6

34. Перечислите факторы, влияющие на выбор компонентов КСЗИ.

35. Опишите объекты защиты как основной фактор, определяющий состав компонентов КСЗИ.

36. Основные требования, предъявляемые к выбору методов и средств защиты, зависимость. их от структуры предприятия, защищаемых элементов объектов, условий функционирования КСЗИ.

37. Опишите процесс проектирования системы защиты информации для существующей АС.

Лекция №7

38. Основные угрозы безопасности информации АС организации.

39. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.

40. Определение потенциальных каналов и методов несанкционированного доступа (НСД) к информации.

41. Определение возможностей НСД к защищаемой информации.

Лекция №8

42. Основные принципы построения комплексной системы защиты информации.

43. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.

Лекция №9

44. Общая характеристика задач моделирования комплексной системы защиты информации.

45. Формальные модели безопасности и их анализ: классификация формальных моделей безопасности; модели обеспечения конфиденциальности; модели обеспечения целостности; субъектно-ориентированная модель.

46. Технологическое и организационное построение КСЗИ.

Лекция №10

47. Кадровое обеспечение функционирования комплексной системы защиты информации.

48. Специфика персонала предприятия как объекта защиты.

49. Распределение функций по защите информации: функции руководства предприятия; функции службы защиты информации; функции специальных комиссий; обязанности пользователей защищаемой информации.

50. Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа.

Лекция №11

51. Состав и значение материально-технического обеспечения функционирования комплексной системы защиты информации.

52. Перечень вопросов ЗИ, требующих документационного закрепления.

Лекция №12

53. Понятие, сущность и цели управления комплексной системы защиты информации.

54. Принципы управления комплексной системы защиты информации.

55. Структура, процессы, функции и задачи управления комплексной системы защиты информации.

Лекция №13

56. Понятие и задачи планирования функционирования комплексной системы защиты информации.

57. Факторы, влияющие на выбор способов планирования.

58. Методы сбора, обработки и изучения информации, необходимой для планирования.

Лекция №14

59. Виды контроля функционирования комплексной системы защиты информации.

60. Цель проведения контрольных мероприятий в комплексной системы защиты информации.

Лекция №15

61. Понятие и основные виды чрезвычайных ситуаций.

62. Технология принятия решений в условиях ЧС.

63. Факторы, влияющие на принятие решений в условиях ЧС.

64. Подготовка мероприятий на случай возникновения ЧС.

Лекция №16

65. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации.

Лекция №17

66. Показатель уровня защищенности, основанный на экспертных оценках.

67. Экономический подход к оценке эффективности комплексной системы защиты информации.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Системы обеспечения комплексной безопасности» предполагает реализацию следующих форм самостоятельной работы студентов:

- проработка конспекта лекций и учебной литературы;
- изучение печатных источников по теме дисциплины;
- изучение профессиональных электронных ресурсов по теме дисциплины;
- изучение вопросов для самоконтроля;
- решение во внеурочное время контрольных задач, получаемых на лекциях;
- углублённое изучение отдельных тем учебной дисциплины для подготовки к устным опросам;
- изучение основной и дополнительной и научной литературы в процессе подготовки к анализу и решению проблемных задач, реализации элементов исследовательской деятельности;
- подготовка к текущей диагностике компетенции (письменным контрольным работам);
- 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 открытых систем автоматизированного тестирования при использовании бесплатного сервиса для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google – Google Класс, которые доступны пользователям через Интернет в любое удобное для них время;
- наличием и полной доступностью электронных вариантов курса лекций и учебно-методических указаний по основным разделам дисциплины на https://moodle.psu.by – образовательном портале Полоцкого государственного университета имени Евфросинии Полоцкой.

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Материалы, размещены на бесплатном сервисе для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google – Google Класс: шифр курса **4CDOKJFJ**.
2. Материалы, размещённые на образовательном портале Полоцкого государственного университета имени Евфросинии Полоцкой **https://moodle.psu.by.**
3. Методические указания к выполнению лабораторных работ по дисциплине «Системы обеспечения комплексной безопасности» для студентов специальности 6-05-0533-12 «Кибербезопасность».

Содержание самостоятельной работы студентов

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины	***Тема 1.1. Сущность и задачи комплексной защиты информации на предприятии.*** Современное понимание методологии защиты информации: особенности национального технического регулирования, современные требования к средствам обеспечения безопасности. Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [5], [7].	4
	Тема 1.3. Факторы, влияющие на организацию комплексной системы защиты информации. Влияние формы собственности на особенности защиты информации ограниченного доступа. Характер основной деятельности предприятия. Структура и территориальное расположение предприятия. Режим функционирования предприятия. Конструктивные особенности предприятия. Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	4
	Тема 2.2. Определение объектов защиты. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие необходимость защиты периметра и здания предприятия. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты. Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [4], [6], [7].	4
	Тема 3.1. Кадровое обеспечение функционирования комплексной системы защиты информации. Специфика персонала предприятия как объекта защиты. Распределение функций по защите информации: функции руководства предприятия; функции службы защиты информации; функции специальных комиссий; обязанности пользователей защищаемой информации. Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	4
	Тема 4.4. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций. Понятие и основные виды чрезвычайных ситуаций. Факторы, влияющие на принятие решений в условиях ЧС. Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	4
	Тема 5.2. Состав методов и моделей оценки эффективности комплексной системы защиты информации. Экономический подход к оценке эффективности комплексной системы защиты информации. Осн. лит.: [1], [4]. Доп. лит.: [1], [3], [7].	4

1	2	3
Подготовка к защите отчетов по лабораторным работам	***Лабораторная работа №1*** Изучение алгоритмов и условия сжатия изображения с видеокамеры.	2
	Лабораторная работа №2 Изучение конструкции, характеристик и принципа работы видеокамер.	2
	Лабораторная работа №3 Проектирование систем видеонаблюдения.	2
	Лабораторная работа №4 Проектировании систем автоматического распознования лиц в видеонаблюдении.	2
	Лабораторная работа №5 Проектирование системы контроля и управления доступом.	2
	Лабораторная работа №6 Изучение средств пожарной сигнализации.	2
	Лабораторная работа №7 Изучение системы для управления информацией и событиями безопасности SIEM (Security Information and Event Management). Моделирование процесса реагирования на киберинциденты с использованием WAZUH.	2
	Лабораторная работа №8 Моделирование процесса реагирования на киберинциденты на примере работы с продуктами компании UserGate.	2
	Лабораторная работа №9 Моделирование процесса реагирования на киберинциденты на примере работы с продуктами компании UserGate.	2
Подготовка к контрольной работе №1		4
Подготовка к контрольной работе №2		4
Подготовка реферативного выступления		6
	ИТОГО:	**56**

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:**

– устная форма (блиц-опрос на лекциях);

– письменная форма (тесты, контрольные работы, письменные отчёты по лабораторным работам);

– устно-письменная форма (отчёты по лабораторным с их устной защитой);

– техническая форма (электронные тесты, визуальные лабораторные работы).

Лабораторный практикум предполагает выполнение и защиту лабораторных работ. Последнее занятие по лабораторному практикуму в семестре предусматривает выполнение и защиту зачетной работы и контрольное тестирование. По каждой лабораторной работе выдается индивидуальное задание. Отчет по лабораторной 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:

$$\text{Т} = \frac{(\text{КТ}_1 + \ldots + \text{КТ}_n) + (\text{КР}_1 + \text{КР}_2) + (\text{ЛР}_1 + \ldots + \text{ЛР}_m)}{(m + n + 2)},$$

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

n – количество тестов;

КР - контрольная работа;

$\text{ЛР}_1 + \ldots + \text{ЛР}_m$ – отметки, выставленные по результатам защит лабораторных работ;

m – количество лабораторных работ.

В таблице 1 представлены составляющие, формирующие отметку текущего контроля Т по дисциплине.

Таблица 1 – Составляющие отметки текущего контроля Т по дисциплине

Мероприятия текущего контроля	**Содержание мероприятий текущего контроля – название раздела (темы)**	**Задания мероприятия текущего контроля**	**Отметка мероприятий текущего контроля (КР), (КТ)**
Контрольная работа №1	*Тема 2.1. Определение и нормативное закрепление состава защищаемой информации.* *Тема 2.2. Определение объектов защиты.* *Тема 2.3. Определение компонентов комплексной системы защиты информации.*	Предлагается три вопроса	Максимальная отметка 10 (десять) баллов
Контрольная работа №2	*Тема 4.4. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций.*	Предлагается три вопроса	Максимальная отметка 10 (десять) баллов

Продолжение таблицы 1

Контрольный тест	Темы и планируемые контрольные тесты указаны в учебно-методической карте дисциплины	Тест ориентирован на прохождение в online-режиме и оформлен в **Google Forms** и размещен в **Google Класс Room**	Максимальная отметка 10 (десять) баллов

Результат текущего контроля рассчитывается как округленное среднее значение.

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 обучающего 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 зачету 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

Основные методы (технологии) обучения, отвечающие целям и задачам учебной дисциплины:

– проблемное обучение (проблемное изложение, вариативное изложение), реализуемое на лекционных занятиях;

– учебно-исследовательская деятельность.

Используемые технологии обучения и диагностики компетенций в преподавании дисциплины «Системы обеспечения комплексной безопасности» реализуют подход, основанный на максимально возможном использовании внутренней и учебной мотивации студента, проявляющейся в чётком 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 «Системы обеспечения комплексной безопасности» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Изучение учебной дисциплины осуществляется на лекционных занятиях, на которых студенты овладевают системой теоретических знаний по решению задач обеспечения комплексной безопасности критически важных объектов информатизации с использованием внутренних ресурсов, современных методов и технологий защиты, включая средства инженерной защиты: систем видеонаблюдения, систем управления и контроля доступа (СКУД), систем охранной и пожарной безопасности и т.д, а также на лабораторных занятиях, на которых развиваются и формируются необходимые практические умения и навыки проектирования и разработки комплексных систем безопасности.

В ходе лекционного изложения теоретических сведений используются традиционные словесные приёмы и методы, которые активизируются постановкой проблемных вопросов и заданий, организацией учебных дискуссий с опорой на имеющуюся начальную подготовку студентов и их политехнический кругозор, использованием интерактивных методов обучения.

Во время проведения лабораторных работ особое внимание уделяется формированию у студентов умения планировать свою работу и определять эффективную последовательность её 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 учреждения высшего образования по учебной дисциплине**	**Решение, принятое кафедрой, разработавшей учебную программу**
Дипломное проектирование	Кафедра математики и компьютерной безопасности	Предложений и замечаний нет	

Заведующий кафедрой математики и компьютерной безопасности, к.т.н., доцент И.Б. Бураченок