МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
Учебно-методическое объединение по образованию
в области информатики и радиоэлектроники

УТВЕРЖДАЮ
Первый заместитель Министра образования
Республики Беларусь
_____ А.Г.Баханович
_____

Регистрационный № _____

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Примерная учебная программа по учебной дисциплине
для специальности
7-06-0611-02 Информационная безопасность

СОГЛАСОВАНО
Председатель Учебно-методического объединения по образованию в области информатики и радиоэлектроники
_____В.А.Богуш
_____

СОГЛАСОВАНО
Начальник Главного управления профессионального образования Министерства образования Республики Беларусь
_____С.Н.Пищов
_____

СОГЛАСОВАНО
Проректор по научно-методической работе Государственного учреждения образования «Республиканский институт высшей школы»
_____ И.В.Титович
_____

Эксперт-нормоконтролер
_____
_____

Минск 2025

СОСТАВИТЕЛИ:
Н.А.Певнева, доцент кафедры информационно-измерительных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент;
О.И.Минченок, старший преподаватель кафедры информационно-измерительных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

РЕЦЕНЗЕНТЫ:
Кафедра «Информационно-измерительная техника и технологии» Белорусского национального технического университета (протокол № 3 от 07.10.2025);
М.Л.Радюкевич, заместитель директора по научной работе Государственного предприятия «Научно-исследовательский институт технической защиты информации», кандидат технических наук

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ПРИМЕРНОЙ:
Кафедрой информационно-измерительных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 2 от 18.09.2025);
Научно-методическим советом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № ___ от _____);
Научно-методическим советом по информационной безопасности Учебно-методического объединения по образованию в области информатики и радиоэлектроники (протокол № 2 от 13.10.2025)

Ответственный за редакцию: С.С.Шишпаронок

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ХАРАКТЕРИСТИКА УЧЕБНОЙ ДИСЦИПЛИНЫ

Примерная учебная программа по учебной дисциплине «Менеджмент информационной безопасности» разработана для учреждений высшего образования, осуществляющих подготовку по специальности 7-06-0611-02 «Информационная безопасность» в соответствии с требованиями образовательного стандарта углубленного высшего образования и примерного учебного плана вышеуказанной специальности.

В условиях цифровизации и роста числа киберугроз учебная дисциплина «Менеджмент информационной безопасности» приобретает особую актуальность. Современные организации сталкиваются с необходимостью защиты конфиденциальных данных, соблюдения нормативных требований и обеспечения устойчивости бизнес-процессов. Изучение данной учебной дисциплины позволяет сформировать системный подход к защите информации, управлению рисками, развить навыки анализа угроз, построения политики безопасности, проведения аудита.

Воспитательное значение учебной дисциплины «Менеджмент информационной безопасности» заключается в формировании у обучающихся математической культуры и научного мировоззрения; развитии исследовательских умений, аналитических способностей, креативности, необходимых для решения научных и практических задач; развитии познавательных способностей и активности: творческой инициативы, самостоятельности, ответственности и организованности; формировании способностей к саморазвитию, самосовершенствованию и самореализации.

Изучение данной учебной дисциплины способствует созданию условий для формирования интеллектуально развитой личности обучающегося, которой присущи стремление к профессиональному совершенствованию, активному участию в экономической и социально-культурной жизни страны, гражданская ответственность и патриотизм.

ЦЕЛЬ, ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель учебной дисциплины: составление комплексных представлений о методологии и системном подходе к управлению информационной безопасностью организаций.

Задачи учебной дисциплины:

изучение требований международных и национальных нормативно-правовых актов в области информационной безопасности;

приобретение знаний в области управления информационной безопасностью информационных систем на основе концепции управления PDCA;

изучение принципов построения систем менеджмента информационной безопасности (СМИБ);

приобретение навыков оценки рисков информационной безопасности;

овладение методами управления СМИБ.

Учебная дисциплина «Менеджмент информационной безопасности» базируется на знаниях, полученных при освоении содержания образовательных программ общего высшего образования. Результаты обучения, полученные при освоении учебной дисциплины, необходимы при написании магистерской диссертации.

ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В результате изучения учебной дисциплины «Менеджмент информационной безопасности» формируется следующая углубленная профессиональная компетенция: проводить аудит безопасности информационных систем, по результатам мониторинга обосновано принимать решения о внесении изменений в систему защиты информации.

В результате изучения учебной дисциплины обучающийся должен:

знать:

основные международные и национальные стандарты, регламентирующие управление информационной безопасностью (ИБ);

современные подходы к управлению ИБ и направления их развития;

принципы построения СМИБ;

уметь:

анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ;

применять процессный подход к управлению ИБ в различных сферах деятельности;

применять методы оценки и анализа рисков ИБ организации и создавать документы по управлению СМИБ;

иметь навык: анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СМИБ.

Примерная учебная программа рассчитана на 90 учебных часов, из них – 34 аудиторных. Примерное распределение аудиторных часов по видам занятий: лекции – 18 часов, практические занятия – 16 часов.

ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН

Наименование раздела, темы	Всего аудиторных часов	Лекции	Лабораторные занятия	Практические занятия
Раздел 1. Основы управления информационной безопасностью	**10**	**8**		**2**
Тема 1. Основные положения информационной безопасности	2	2		
Тема 2. Нормативно-правовая база информационной безопасности	4	2		2
Тема 3. Обеспечение информационной безопасности	4	4		
Раздел 2. Концепция управления информационной безопасностью	**24**	**10**		**14**
Тема 4. Система менеджмента информационной безопасности	10	4		6
Тема 5. Управление рисками информационной безопасности	10	4		6
Тема 6. Оценка деятельности по управлению информационной безопасностью	4	2		2
Итого:	**34**	**18**	**-**	**16**

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Тема 1. ОСНОВНЫЕ ПОЛОЖЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение в учебную дисциплину. Цель и задачи учебной дисциплины, ее структура и содержание. Порядок освоения учебной дисциплины. Рекомендуемая литература.

Основные понятия ИБ: «информация», «информационная безопасность», «защита информации», «менеджмент информационной безопасности».

Объекты и субъекты информационной безопасности. Активы, угрозы, уязвимости. Нарушители безопасности информации. Модель нарушителя. Классификация и способы перечисления угроз. Основные методы обеспечения информационной безопасности.

Тема 2. НОРМАТИВНО-ПРАВОВАЯ БАЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Государственная политика в области информационной безопасности. Нормативно-правовые акты в сфере защиты информации и менеджмента информационной безопасности. Концепция информационной безопасности.

Международные стандарты в области информационной безопасности: COBIT, ISO/IEC серии 27000, ISO/IEC 15408, NIST серии 800. Библиотека ITIL.

Требования национальных стандартов в области информационной безопасности: СТБ ISO/IEC 27001, 27002, 27004, 27005; СТБ 34.101.1–3, СТБ 34.101.42, 61, 68, 70.

Тема 3. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные методы обеспечения информационной безопасности.

Системы обнаружения и предотвращения компьютерных атак. Взаимодействие персонала и систем обнаружения и предотвращения компьютерных атак.

Обеспечение конфиденциальности информации: идентификация, аутентификация. Криптографические методы обеспечения конфиденциальности.

Обеспечение целостности информации: корректность транзакций, аутентификация и авторизация пользователей, минимизация привилегий и др. Криптографические методы обеспечения целостности информации. Электронная цифровая подпись.

Обеспечение доступности информации: дублирование, резервирование, избыточность каналов связи, балансировка нагрузки и др. Организация хранения информации.

Раздел 2. КОНЦЕПЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Тема 4. СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Понятие процессного подхода. Цикл Деминга (PDCA). Основные процессы системы менеджмента информационной безопасности и требования, предъявляемые к ним, в соответствии с СТБ ISO/IEC 27001.

Понятие политики информационной безопасности, ее цели. Структура и содержание политики информационной безопасности. Источники информации для разработки политики информационной безопасности. Частные политики информационной безопасности. Процедуры, регламенты и инструкции по информационной безопасности.

Тема 5. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные определения и цель анализа рисков информационной безопасности.

Понятие, типы и инвентаризация активов. Идентификация требований законодательства и бизнеса. Определение угроз и уязвимостей. Оценка рисков ИБ. Количественный и качественный подходы к оценке рисков ИБ. Способы обработки рисков. Выбор и реализация мер и средств безопасности. Мониторинг и пересмотр рисков ИБ.

Процессная модель управления рисками.

Концепции управления рисками информационной безопасности на основе ISO/IEC 27005, COBIT, COBRA, NIST и др.

Инструментальные средства анализа рисков ИБ (COBRA, RA Sofware, CRAMM, RiskWatch и т.д.).

Тема 6. ОЦЕНКА ДЕЯТЕЛЬНОСТИ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Процессы проверки СМИБ (мониторинг, аудит, анализ СМИБ руководством организации, инструментальные средства проверки ИБ).

Цели и задачи аудита СМИБ. Критерии аудита. Основные этапы проведения аудита.

Оценка деятельности по управлению ИБ (оценка эффективности и результативности деятельности по управлению ИБ, измерения, показатели).

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

ОСНОВНАЯ

1. Белявский, Д. А. Управление информационной безопасностью : учебник / Д. А. Белявский, А. С. Кабанов, А. Б. Лось ; под общ. ред. А. В. Сахарова. – Москва : Академия, 2022. – 176 с.

2. Милославская, Н. Г. Управление рисками информационной безопасности : учебное пособие / Н. Г. Милославская, А. И. Толстой. – Москва : Горячая линия-Телеком, 2023. – 224 с.

3. Николаев, Н. С. Управление информационной безопасностью : учебник / Н. С. Николаев. – Москва : Кнорус, 2021. – 190 с.

ДОПОЛНИТЕЛЬНАЯ

4. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : решение Всебелорусского народного собрания от 25 апреля 2024 г. № 5. Режим доступа : https://pravo.by/document/?guid=3871&p0=p924v0005. – Дата доступа: 07.10.2025.

5. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета безопасности Респ. Беларусь от 18 марта 2019 г. № 1. Режим доступа : https://pravo.by/document/?guid=3871&p0=p219s0001. – Дата доступа: 07.10.2025.

6. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь от 10 ноября 2008 г. № 455-З. Режим доступа : https://pravo.by/document/?guid=3871&p0=h10800455. – Дата доступа: 07.10.2025.

7. О совершенствовании государственного регулирования в области защиты информации [Электронный ресурс] : Указ Президента Респ. Беларусь от 9 декабря 2019 г. № 449. Режим доступа : https://pravo.by/document/?guid=12551&p0=P31900449. – Дата доступа: 07.10.2025.

8. Об изменении приказов Оперативно-аналитического центра при Президенте Республики Беларусь от 28 марта 2014 г. № 26 и от 20 февраля 2020 г. № 66 [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 10 декабря 2024 г. № 259. Режим доступа : https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2024-259.pdf. – Дата доступа: 07.10.2025.

9. СТБ ISO/IEC 27001-2024 Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования.

10. СТБ ISO/IEC 27002-2024 Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью.

11. СТБ ISO/IEC 27003-2014 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности.

12. СТБ ISO/IEC 27004-2014 Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

13. СТБ ISO/IEC 27005-2024 Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по менеджменту рисков информационной безопасности.

14. СТБ 34.101.1-2014 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

15. СТБ 34.101.2-2014 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

16. СТБ 34.101.3-2014 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности.

17. СТБ 34.101.41-2013 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения.

18. СТБ 34.101.42-2013 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности.

19. СТБ 34.101.61-2013 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки рисков нарушения информационной безопасности.

20. СТБ 34.101.68-2013 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки соответствия информационной безопасности банков Республики Беларусь требованиям СТБ 34.101.41.

21. СТБ 34.101.70-2016 Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах.

22. Основы управления информационной безопасностью : учебное пособие / А. П. Курило [и др.]. – Москва : Горячая линия-Телеком, 2014. – 244 с.

23. Милославская, Н. Г. Управление информационной безопасностью: Конспект лекций : учебное пособие / Н. Г. Милославская, А. И. Толстой. – Москва : НИЯУ МИФИ, 2020. – 536 с.

24. Милославская, Н. Г. Проверка деятельности по управлению информационной безопасностью : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия-Телеком, 2014. – 186 с.

25. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. – Санкт-Петербург : Лань, 2024. – 324 с.

26. Цирлов, В. Л. Основы информационной безопасности автоматизированных систем / В. Л. Цирлов. – Ростов-на-Дону : Феникс, 2008. – 254 с.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

При изучении учебной дисциплины рекомендуется использовать следующие формы самостоятельной работы:

конспектирование;

реферирование литературы;

выполнение заданий поисково-исследовательского характера;

выполнение расчетов;

подготовка докладов, сообщений, рефератов.

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ КОМПЕТЕНЦИЙ ОБУЧАЮЩИХСЯ

Примерным учебным планом по специальности 7-06-0611-02 «Информационная безопасность» в качестве формы промежуточной аттестации по учебной дисциплине «Менеджмент информационной безопасности» рекомендуется экзамен. Оценка учебных достижений обучающихся производится по десятибалльной шкале.

Для текущего контроля по учебной дисциплине и диагностики компетенций могут использоваться следующие формы:

текущий опрос;

тестирование;

контрольная работа;

отчеты по практическим занятиям с их устной защитой;

групповые проекты.

РЕКОМЕНДУЕМЫЕ МЕТОДЫ (ТЕХНОЛОГИИ) ОБУЧЕНИЯ

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

проблемное обучение (проблемное изложение, вариативное изложение, частично-поисковый метод), реализуемое на лекционных занятиях;

учебно-исследовательская деятельность, творческий подход, реализуемые на практических занятиях.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

1. Нормативно-правовая база управления информационной безопасностью.
2. Идентификация и оценка угроз и уязвимостей информационной безопасности.
3. Оценка рисков.
4. Инструментальные средства анализа рисков ИБ.
5. Проектирование модели PDCA для СМИБ.

6. Проектирование системы менеджмента информационной безопасности.
7. Проектирование систем защиты информации.
8. Политика информационной безопасности организации.
9. Аудит информационной безопасности.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ПРОГРАММ
(*необходимого оборудования, наглядных пособий и др.)*

1. MSAT (Microsoft Security Assessment Tool).
2. OWASP Risk Rating Methodology.
3. Ra2.
4. VsRisk.
5. Risk Assessment Excel Templates.