**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

Учебно-методическое объединение по образованию в области управления

**УТВЕРЖДАЮ**

Первый заместитель Министра образования Республики Беларусь

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.А.Старовойтова

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Регистрационный № ТД- \_\_\_\_\_ /тип.

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**

**Типовая учебная программа по учебной дисциплине**

**для направления специальности**

**1-26 02 04-02 Документоведение (информационное обеспечение управления)**

|  |  |
| --- | --- |
| **СОГЛАСОВАНО**Председатель Учебно-методического объединения по образованию в области управления\_\_\_\_\_\_\_\_\_\_\_\_\_ Г.В.Пальчик \_\_\_\_.\_\_\_\_.\_\_\_\_\_\_\_\_.**СОГЛАСОВАНО**Директор Департамента по архивам и делопроизводству Министерства юстиции Республики Беларусь\_\_\_\_\_\_\_\_\_\_\_\_\_ В.И.Кураш\_\_\_\_.\_\_\_\_.\_\_\_\_\_\_\_\_. | **СОГЛАСОВАНО**Начальник Главного управления профессионального образования Министерства образования Республики Беларусь \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.А.Касперович\_\_\_\_.\_\_\_\_.\_\_\_\_\_\_\_\_.Проректор по научно-методической работе Государственного учреждения образования «Республиканский институт высшей школы»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.В.Титович\_\_\_\_.\_\_\_\_.\_\_\_\_\_\_\_\_. |
|  | Эксперт-нормоконтролёр\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.\_\_\_\_.\_\_\_\_\_\_\_\_. |

Минск 201\_\_

**Составители:**

**В.И. Бобышев**, доцент кафедры источниковедения Белорусского государственного университета, кандидат исторических наук;

**А.М. Назаренко**, старший преподаватель кафедры источниковедения Белорусского государственного университета.

Рецензенты:

**Кафедра экономики и управления** Частного учреждения образования «Институт парламентаризма и предпринимательства»;

**А.Е. Рыбаков,** директор учреждения «Белорусский научно-исследовательский институт документоведения и архивного дела», кандидат исторических наук, доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:

Кафедрой источниковедения Белорусского государственного университета

(протокол №9 от 06.04.2018);

Научно-методическим советом Белорусского государственного университета

(протокол №6 от 16.06.2018);

Президиумом Совета Учебно-методического объединения по образованию в области управления (протокол № 3 от 09.01.2019).

**Ответственный за редакцию:** В.И. Бобышев

**Ответственный за выпуск**: А.М. Назаренко

**1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

Типовая учебная программа по дисциплине «Информационная безопасность и защита информации» предназначена для усвоения на первой ступени высшего образования студентами, обучающимися по направлению специальности 1-26 02 04-02 «Документоведение (информационное обеспечение управления)» в учреждениях высшего образования Республики Беларусь.

Вопросы защиты информации в современном обществе занимают ключевое место и охватывают экономическую, политическую, социальную сферы деятельности. Распространение компьютерных технологий в повседневной работе организаций, расширение сферы использования автоматизированных систем в документационном обеспечении управления изменили характер и диапазон вопросов обеспечения информационной безопасности и защиты информации. Сегодня защита информации не является односторонней проблемой, а представляет собой сложный комплекс технических, организационных, правовых методов и средств защиты.

Дисциплина «Информационная безопасность и защита информации» относится к дисциплинам направления специальности обязательного компонента цикла специальных дисциплин. Изучение информационной безопасности и защиты информации основывается на знаниях и умениях, приобретённых при изучении таких дисциплин как «Основы информационных технологий», «Документоведение», «Технология и организация документационного обеспечения управления», «История и современная организация государственных учреждений Беларуси», «Правоведение». Результаты изучения информационной безопасности способствуют успешному овладению программами курсов «Менеджмент», «Организационное проектирование», ряда курсов цикла дисциплин специализации, имеют существенное значение для качественного выполнения курсовых работ и выпускной квалификационной работы.

Дисциплина «Информационная безопасность и защита информации» может быть рекомендована для изучения в качестве дисциплины вузовского компонента либо дисциплины по выбору студента для направления 1-26 02 04-01 «Документоведение (документационное обеспечение управления)», а также для студентов иных специальностей соответствующего профиля.

**Основной целью изучения дисциплины** является формирование системы комплексных теоретических знаний, практических умений и навыков в области создания и управления системами информационной безопасности организаций.

**Основными задачами изучения дисциплины являются:**

* усвоение содержания основных понятий в области информационной безопасности и защиты информации;
* формирование системы знаний о правом регулировании в области информационной безопасности и защиты информации;
* формирование знаний и умений по защите информации при осуществлении различных видов деятельности.

В результате изучения дисциплины студент **должен** **знать:**

* сущность, цели и принципы, конституционные и законодательные основы национальной безопасности Республики Беларусь в информационной сфере, направления её обеспечения, государственную политику в области информационной безопасности;
* организационно-правовые аспекты информационной безопасности;
* основные направления и методы защиты вычислительной, организационной техники и сетей, средств связи от технических средств промышленного шпионажа;

**уметь:**

* использовать методику защиты информации при проведении основных деловых мероприятий, в научной деятельности, работе кадровой службы и др.;
* осуществлять организационно-правовое обеспечение функционирования и совершенствования систем защиты информации, служб безопасности, конфиденциальной документации, персонала;

**владеть:**

* методами обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению соответствующих угроз;
* методами работы с персоналом, который обладает конфиденциальной информацией;
* навыками организации и ведения конфиденциального делопроизводства.

Учебная дисциплина способствует формированию следующих академических,социально-личностных и профессиональных компетенций согласно образовательному стандарту по указанной специальности.

**Академические компетенции (АК):**

АК-1. Уметь использовать базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-6. Владеть междисциплинарным подходом при решении проблем.

АК-7. Уметь собирать, систематизировать информацию и управлять ей.

АК-8. Иметь навыки, связанные с использованием технических средств, управлением информацией и работой с компьютером.

АК-9. Владеть государственными языками (белорусским и русским), одним или несколькими иностранными языками на уровне, достаточном для эффективной письменной и устной профессиональной и межличностной коммуникации.

АК-10. Уметь учиться, повышать свою квалификацию в течение всей жизни.

АК-11. Уметь самостоятельно принимать профессиональные решения с учётом их социальных и экологических последствий.

АК-12. Анализировать исторические и современные проблемы экономической и социальной жизни общества.

**Социально-личностные компетенции (СЛК):**

СЛК-1. Обладать качествами гражданственности.

СЛК-2. Быть способным к социальному взаимодействию.

СЛК-3. Обладать способностью к межличностным коммуникациям.

СЛК-5. Быть способным к критике и самокритике (критическое мышление).

СЛК-6. Уметь работать в команде.

СЛК-7. Быть способным к самостоятельному обучению.

СЛК-8. Уметь формировать собственное мнение.

СЛК-9. Иметь навыки публичных выступлений и презентаций.

СЛК-10. Быть способным использовать полученные знания.

**Профессиональные** **(ПК):**

ПК-1. Планировать, организовывать и совершенствовать деятельность служб документационного, информационного обеспечения управления.

ПК-4. Разрабатывать проекты решений и организовывать их обсуждение.

ПК-6. Формулировать задачи по проектированию, эксплуатации и совершенствованию (в части информационного обеспечения) автоматизированных информационных систем и систем управления, принимать участие в разработке новейших информационных технологий.

ПК-7. Разрабатывать предложения по обеспечению эргономичных условий труда, рационализации рабочих мест работников службы документационного обеспечения управления.

ПК-8. Диалектически мыслить и аргументировать свою точку зрения, анализировать факты и прогнозировать развитие событий, разрабатывать решения с учётом экономических, социальных и этических требований, оценивать исторические и современные проблемы и тенденции.

ПК-9. Готовить научные материалы, представлять итоги проделанной работы в виде отчётов, рефератов, статей, рецензий, оформленных в соответствии с имеющимися требованиями с привлечением современных информационных технологий и средств организационной техники.

ПК-10. Избирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования.

ПК-13. Уметь пользоваться научной и справочной литературой на разных языках.

ПК-14. Участвовать в практической реализации поддержки процессов управления документами, профессионально применять современное оборудование и инструменты.

ПК-19. Творчески применять полученные знания и приобретённые навыки в профессиональной деятельности.

ПК-24. Осуществлять документационное обеспечение деятельности по управлению интеллектуальной собственностью.

Учебная дисциплина рассчитана на 110 часов, из них 68 аудиторных часов (примерное распределение по видам занятий: лекции –44 часа, семинарские занятия – 22 часа).

**2. ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН**

|  |  |  |
| --- | --- | --- |
| **№****п/****п**  | **Название разделов, тем** | **Количество часов** |
| **Аудиторных** | **В том числе** |
| Лекции | Семинарские занятия |
| **РАЗДЕЛ І. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ И ЗАЩИТУ ИНФОРМАЦИИ** |  |  |  |
| 1 | Основы теории и методологии информационной безопасности и защиты информации | 4 | 2 | 2 |
| 2 | Основные направления обеспечения защиты информационных ресурсов | 2 | 2 |  |
| 3 | Легальные и незаконные способы получения полезной и конфиденциальной информации | 2 | 2 |  |
| РАЗДЕЛ ІІ. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ |  |  |  |
| 4 | Основы информационного права | 4 | 2 | 2 |
| 5 | Правовой режим государственных секретов в Республике Беларусь | 4 | 2 | 2 |
| 6 | Правовой режим коммерческой тайны в Республике Беларусь | 4 | 2 | 2 |
| 7 | Правовой режим профессиональных тайн, личной тайны и персональных данных в Республике Беларусь | 4 | 2 | 2 |
| РАЗДЕЛ ІІІ. ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ |  |  |  |
| 8 | Организационные меры защиты информации | 2 | 2 |  |
| 9 | Аналитическая работа при обеспечении информационной безопасности | 2 | 2 |  |
| 10 | Организация работы с персоналом, обладающим конфиденциальной информацией  | 2 | 2 |  |
| 11 | Защита информации при проведении совещаний и переговоров | 2 | 2 |  |
| 12 | Защита информации в процессе научной, рекламной и выставочной деятельности | 2 |  | 2 |
| 13 | Организация защиты информации в процессе сотрудничества, порядок работы с клиентами и посетителями | 2 |  | 2 |
| 14 | Деятельность служб безопасности в области защиты информации | 2 |  | 2 |
| **РАЗДЕЛ IV. КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО** |  |  |  |
| 15 | Понятие конфиденциального делопроизводства и методологические основы его организации  | 2 | 2 |  |
| 16 | Технологические системы защиты, обработки и хранения конфиденциальных документов | 2 | 2 |  |
| 17 | Учёт конфиденциальных документов | 2 | 2 |  |
| 18 | Документирование конфиденциальной информации | 4 | 2 | 2 |
| 19 | Накопление конфиденциальных документов в процессе работы и организация их архивного хранения | 2 | 2 |  |
| 20 | Организационные аспекты уничтожения конфиденциальных материалов  | 2 | 2 |  |
| 21 | Порядок работы персонала с конфиденциальными материалами | 4 | 2 | 2 |
| 22 | Контроль за обеспечением конфиденциального делопроизводства | 2 | 2 |  |
| **РАЗДЕЛ V. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ** |  |  |  |
| 23 | Технические меры защиты информации | 6 | 4 | 2 |
| 24 | Основы защиты информации в компьютерах, локальных сетях и средствах связи | 4 | 2 | 2 |
| **Всего** | **68** | **44** | **24** |

**3. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**РАЗДЕЛ I. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ**

**И ЗАЩИТУ ИНФОРМАЦИИ**

**Тема 1. Основы теории и методологии информационной безопасности и защиты информации**

Предмет дисциплины «Информационная безопасность и защита информации». Цель и задачи курса. Место дисциплины в системе подготовки специалиста. Структура и содержание курса. Характеристика основной
и дополнительной литературы.

Понятие безопасности. Национальная безопасность. Информационная безопасность в системе национальной безопасности Республики Беларусь. Основные понятия, общеметодологические принципы теории информационной безопасности. Национальные интересы Республики Беларусь в информационной сфере. Угрозы национальной безопасности в информационной сфере и их источники. Система обеспечения информационной безопасности в Республике Беларусь. Государственная информационная политика. Государственные органы Республики Беларусь, выполняющие функции обеспечения информационной безопасности и защиты информации.

Понятие защиты информации. Соотношение понятий информационной безопасности и безопасности информации. Виды информации, методы, средства и способы ее защиты. Методы нарушения конфиденциальности, целостности и доступности информации. Источники утраты конфиденциальности и искажения информации.

Понятие информационного противоборства, его виды. Формы, методы и способы информационного противоборства. Информационные войны и их источники. Конкуренция и соперничество в области информационных технологий. Противодействие использованию информационных технологий в преступных целях.

**Тема 2. Основные направления обеспечения защиты информационных ресурсов**

Понятие и виды информационных ресурсов. Защита информационных ресурсов. Критерии классификации информационных ресурсов. Понятие тайны (государственная, служебная, коммерческая, профессиональная, банковская, личная, семейная и др.) и секрета (государственные секреты, «фирменные», технологические (ноу-хау), научные (ноу-ноу) и др.). Понятие конфиденциальности. Критерии выделения информации ограниченного доступа. Виды конфиденциальной информации. Понятие уязвимости информации. Угрозы информации. Система защиты информационных ресурсов. Документирование как обязательное условие включения информации в информационные ресурсы. Особенности документирования конфиденциальной информации.

**Тема 3. Легальные и незаконные способы получения полезной и конфиденциальной информации**

Понятие и методы информационно-аналитической работы. Понятие источника информации и его виды. Критерии аналитической оценки информации. Аналитическая разведка. Бизнес-разведка. Экономическая и коммерческая разведка. Основы проведения аналитических исследований.

Формы недобросовестной конкуренции и соперничества. Классификация противоправных способов получения конфиденциальной информации. Понятие шпионажа и его виды. Коммерческий шпионаж и его формы. Разглашение информации персоналом, его причины и формы.

**РАЗДЕЛ II. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ**

**Тема 4. Основы информационного права**

Понятие информационного права. Предмет, методы и принципы информационного права. Система информационного права. Институты информационного права. Информационно-правовые отношения. Виды информационно-правовых норм. Законодательство Республики Беларусь в области информационной безопасности и защиты государственных секретов.

Понятие правового режима информации и его виды. Понятие и виды информации ограниченного распространения. Правовые способы обеспечения защиты информации. Юридическая ответственность в области информационных отношений. Преступления в информационной сфере: понятие, характеристика основных составов, особенности расследования.

**Тема 5. Правовой режим государственных секретов в Республике Беларусь**

Понятие и виды государственных секретов в Республике Беларусь. Правовой режим государственной тайны. Правовой режим служебной тайны. Сведения, которые не могут быть отнесены к государственным секретам. Допуск и доступ к государственным секретам. Законодательство Республики Беларусь в области государственных секретов. Юридическая ответственность за утрату государственных секретов. Международное сотрудничество в области информационной безопасности и защиты информации.

**Тема 6. Правовой режим коммерческой тайны в Республике Беларусь**

Понятие коммерческой тайны в Республике Беларусь. Признаки коммерческой тайны. Условия правовой защиты коммерческой тайны. Сведения, которые не могут составлять коммерческую тайну. Допуск и доступ к коммерческой тайне. Законодательство Республики Беларусь в области коммерческой тайны. Юридическая ответственность за утрату коммерческой тайны. Использование коммерческой тайны в хозяйственной деятельности юридических лиц и основы обеспечения ее защиты.

**Тема 7. Правовой режим профессиональных тайн, личной тайны и персональных данных в Республике Беларусь**

Понятие профессиональных тайн и их виды (медицинская (врачебная) тайна, банковская тайна, тайна страхования, нотариальная тайна, тайна следствия, адвокатская тайна, тайна исповеди и другие). Особенности правового режима профессиональных тайн. Основания и условия защиты профессиональных тайн. Особенности допуска и доступа различным видам профессиональных тайн. Законодательство Республики Беларусь в отношении различных видов профессиональных тайн. Особенности юридической ответственности за утрату различных видов профессиональных тайн. Особенности использования профессиональных тайн в процессе различных видов деятельности.

Понятие личной тайны. Конституционные основы защиты неприкосновенности частной жизни человека. Условия правовой защиты личной тайны. Юридическая ответственность за утрату личной тайны.

Понятие персональных данных. Особенности правового режима персональных данных. Законодательство Республики Беларусь в области персональных данных. Использование персональных данных
в различных видах деятельности.

**РАЗДЕЛ III. ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ**

**Тема 8. Организационные меры защиты информации**

Понятие и виды организационных мер обеспечения информационной безопасности и защиты информации. Анализ и оценка угроз информационной безопасности объекта. Понятие и виды ущерба. Средства и методы физической защиты объектов. Организация обеспечения режима конфиденциальности. Регламентация допуска и доступа персонала к конфиденциальной информации.

**Тема 9. Аналитическая работа при обеспечении информационной безопасности**

Понятие и методы информационно-аналитической работы. Цели, задачи и направления информационно-аналитической работы на объекте. Организация информационно-аналитических структур, их функции и задачи. Виды информационно-аналитических документов и особенности их подготовки. Аналитическое исследование и мониторинг угроз информационной безопасности на объекте. Выявление каналов несанкционированного доступа и утечки информации. Прогнозирование обстановки (внутренней и внешней среды) в процессе обеспечения информационной безопасности объекта. Порядок и способы сбора первичной информации, критерии ее оценки. Выдвижение версий и гипотез, проведение их проверки. Подготовка экспертных оценок и заключений. Выработка предложений и рекомендаций.

**Тема 10. Организация работы с персоналом, обладающим конфиденциальной информацией**

Психологические особенности человека, владеющего тайной. Задачи и способы подбора персонала на работу, связанную и использованием конфиденциальной информации. Методы сбора информации о кандидатах на работу, этапы и процедуры их проверки. Источники информации о личных и деловых качествах кандидата на работу, особенности документирования результатов проверочных мероприятий. Способы и формы проведения анкетирования, тестирования, опроса, персонального собеседования. Особенности документирования приёма лиц на работу, связанную с допуском к конфиденциальной информации. Виды и формы закрепления обязательств о неразглашении конфиденциальных сведений. Оформление допуска сотрудника к конфиденциальным сведениям.

Направления, методы и особенности работы с категориями сотрудников, допущенных к конфиденциальной информации. Принципы, организационные формы и методика обучения сотрудников правилам обеспечения безопасности информации. Методика проведения инструктирования сотрудников. Формы и методы индивидуальной работы с сотрудниками. Порядок обучения персонала правилам поведения в различных экстремальных ситуациях. Методы контроля за соблюдением персоналом правил работы с конфиденциальной информацией. Порядок проведения служебного расследования по фактам разглашения или утечки конфиденциальной информации, утраты документов и носителей информации. Цели и формы морального и материального стимулирования ответственного отношения сотрудников к работе с конфиденциальной информацией. Роль психологического климата. Предупредительные и профилактические меры. Перевод и увольнение сотрудников, допущенных к конфиденциальной информации (особенности документирования). Процедура и формы превентивного контроля за сотрудниками после увольнения.

**Тема 11. Защита информации при проведении совещаний и переговоров**

Совещания как форма управленческой деятельности. Виды совещаний. Переговоры как вид управленческой деятельности. Виды и формы переговоров. Стратегия и тактика переговорного процесса.

Общие требования соблюдения конфиденциальности при подготовке конфиденциальных совещаний и переговоров. Порядок и принципы отбора информации для обсуждения, способы её доведения до участников.

Документирование конфиденциальной информации в ходе совещаний и переговоров. Подготовка и оформление стенограмм, протоколов, итоговых документов. Регламентирование процедур аудио- и видеозаписи в ходе проведения конфиденциальных совещаний и переговоров. Инженерно-технические требования к помещениям, организация внешней и внутренней охраны. Обязанности участников совещаний и переговоров, а также лиц, ответственных за их проведение. Угрозы безопасности информации при подготовке и проведении конфиденциальных совещаний и переговоров. Задачи и способы защиты конфиденциальных сведений в ходе совещаний.

**Тема 12. Защита информации в процессе научной, рекламной и выставочной деятельности**

Виды научных публикаций. Особенности использования результатов научных исследований, содержащих сведения конфиденциального характера. Принципы и методы комплексного анализа ценности информации, содержащийся в научных трудах. Методы защиты ценных элементов идей и решений.

Виды рекламной деятельности, особенности использования информации в различных видах рекламной продукции. Оформление разрешения на издание рекламной продукции. Анализ рекламной продукции на предмет возможного разглашения ценных сведений.

Виды выставочной деятельности и презентация продукции. Оформление разрешения на демонстрацию продукции, технической документации и моделей. Методы подготовки сотрудников по вопросам защиты ценной информации. Организация работы с персоналом в ходе проведения выставок. Угрозы безопасности информации в процессе научной, рекламной и выставочной деятельности. Задачи и способы защиты информации. Контроль эффективности защиты информации.

**Тема 13. Организация защиты информации в процессе сотрудничества, порядок работы с клиентами и посетителями**

Основные задачи защиты конфиденциальных сведений при работе с клиентами и посетителями. Классификация посетителей. Правила работы с различными группами посетителей. Организация приема клиентов и посетителей. Обязанности лиц, ответственных за приём клиентов и посетителей. Методы контроля за поведением клиентов и посетителей. Оборудование помещений и мест для приёма клиентов и посетителей. Угрозы безопасности информации при работе с клиентами и посетителями. Способы обеспечения защиты конфиденциальных сведений при работе с клиентами и посетителями.

**Тема 14. Деятельность служб безопасности в области защиты информации**

Правовая регламентация охранной деятельности в Республике Беларусь. Служба безопасности, её структура и задачи по обеспечению информационной безопасности. Задачи и организация работы службы безопасности
с персоналом. Взаимодействие службы безопасности с правоохранительными органами.

Виды охраняемых объектов, категории защищаемых помещений. Задачи и организационные формы охраны объектов. Построение системы охраны объекта, многорубежная охрана. Пропускной режим и контроль на объекте. Использование технических средств службой безопасности в процессе выполнения рабочих задач. Технические средства идентификации. Правила охраны транспортных средств и транспортируемой продукции. Правила личной охраны персонала. Классификация экстремальных (чрезвычайных) ситуаций. Защита объекта и информации в экстремальных ситуациях.

**РАЗДЕЛ IV. КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО**

**Тема 15. Конфиденциальный документооборот и обеспечение его защиты**

Понятие конфиденциального (защищённого) документооборота. Виды угроз традиционным и электронным документам. Задачи защиты документопотоков. Критерии безопасности документооборота. Основные требования к защищённому документообороту. Взаимосвязь персональной избирательности в доставке информации и разрешительной системы доступа. Особенности защищённого электронного документооборота. Типовая структура технологических стадий входного, выходного и внутреннего потоков конфиденциальных документов. Принципиальная взаимосвязь документопотока и применяемой технологической системы обработки и хранения документов.

**Тема 16. Технологические системы защиты, обработки и хранения конфиденциальных документов**

Понятие технологической системы обработки и хранения конфиденциальных документов. Виды угроз документированной информации, исходящие от технологической системы обработки и хранения конфиденциальных документов в системе защиты информации и защищённом документообороте. Организационные и технологические требования к обработке и хранению конфиденциальных документов. Единство научных и методических основ обработки и хранения открытых и конфиденциальных документов. Преимущества и недостатки традиционной технологической системы. Принципиальные особенности автоматизированной технологической системы обработки конфиденциальных документов. Системы автоматизации одного рабочего места по работе с конфиденциальными документами. Возможности создания различных типов АСОД для конфиденциальных документов – электронного документооборота на базе компьютерных сетей.

**Тема 17. Учёт конфиденциальных документов**

Основные элементы и стадии технологии обработки поступивших конфиденциальных документов. Угрозы документам в процессе учёта. Цели и задачи учёта конфиденциальных документов и носителей конфиденциальной информации, специфические принципы учёта. Виды учёта, их место в технологической системе обработки и хранения конфиденциальных документов. Информационная взаимосвязь отдельных видов учёта документов. Состав процедур традиционного учёта документов. Функции и структура традиционного справочно-информационного банка данных по документам (журналов учёта бумажных и электронных носителей, контрольных журналов и картотек). Состав процедур автоматизированного учёта бумажных и электронных конфиденциальных документов. Функции автоматизированного справочно-информационного банка данных по документам. Правила применения цифровой электронной подписи. Назначение и процедуры учёта поступивших конвертов, пакетов. Назначение и процедуры учёта поступивших подготовленных конфиденциальных документов. Инвентарный учёт конфиденциальных документов. Учёт носителей конфиденциальной информации. Учёт законченных производством дел, содержащих конфиденциальные документы, учёт картотек и журналов учёта документов. Способы защиты конфиденциальных документов и их носителей в процессе технологии их обработки.

**Тема 18. Документирование конфиденциальной информации**

Понятие документирования конфиденциальной информации. Принципы документирования конфиденциальной информации. Критерии отнесения документов к категории конфиденциальных. Перечень конфиденциальных документов, содержащих сведения, представляющие коммерческую тайну. Составление и ведение перечня конфиденциальных документов. Этапы подготовки (исполнения) конфиденциальных документов: 1) определения уровня грифа конфиденциальности предполагаемого документа; 2) предварительного учёта бумажных и технических носителей конфиденциальной информации; 3) составления конфиденциального документа; 4) изготовления оригинала конфиденциального документа; 5) издания подготовленных конфиденциальных документов. Порядок копирования и тиражирования конфиденциальных документов. Особенности конвертования (пакетирования) отправляемых конфиденциальных документов, доставки их адресатам. Особенности направления на исполнение изданных внутренних документов. Особенности передачи адресатам по незащищённым линиям связи факсимильных, электронных документов, телеграмм, телексов. Угрозы информации при документировании и задачи её защиты. Угрозы изданным документам и задачи их защиты. Способы защиты конфиденциальной информации в процессе документирования.

**Тема 19. Формирование конфиденциальных документов в дела, хранение дел и передача их в архив.**

Процедура составления, ведения и закрытия номенклатуры дел. Порядок формирования дел. Особенности оформления дела при его заведении и формировании. Правила формирования и хранения дел с конфиденциальными документами. Особенности оформления дела при его закрытии. Назначение и задачи учёта законченных производством дел, картотек и журналов. Особенности экспертизы ценности конфиденциальных документов и процедуры составления описи дел, передаваемых в архив. Порядок хранения дел в службе конфиденциальной документации и архиве. Классификация и учёт архивных дел, научно-справочный аппарат, организация использования документов и дел. Угрозы документам в процессе формирования их в дела и хранения. Задачи и способы защиты конфиденциальной информации.

**Тема 20. Уничтожение документов, дел и носителей информации**

Общие особенности уничтожения конфиденциальных документов. Процедура составления акта на уничтожение конфиденциальных документов и дел. Состав документов, проектов документов, других материалов и носителей информации, уничтожаемых без акта. Процедура физического уничтожения документов и её документирование. Угрозы документам в процессе уничтожения. Задачи и способы защиты конфиденциальной информации в процессе уничтожения документов.

**Тема 21. Порядок работы персонала с конфиденциальными документами и материалами**

Условия и порядок получения доступа персонала к конфиденциальным документам и материалам. Ознакомление сотрудников с нормативно-правовой базой, устанавливающей порядок работы с конфиденциальными документами и материалами. Соблюдение должностных инструкций – главное требование при работе с конфиденциальной информацией. Ответственность сотрудников за нарушение правил работы с конфиденциальными документами и материалами. Действия сотрудников при получении конфиденциальных документов для работы. Порядок использования конфиденциальных документов и материалов в процессе выполнения должностных обязанностей. Действия персонала при документировании конфиденциальной информации. Порядок возвращения документов и материалов в службу конфиденциального документооборота. Угрозы конфиденциальным документам при работе с ними персонала. Задачи и способы защиты информации при работе сотрудников с конфиденциальными документами и материалами.

**Тема 22. Проверка наличия документов, дел и носителей информации**

Назначение, задачи и типы проверок наличия конфиденциальных документов, дел и носителей информации. Методика ведения проверки наличия документов. Ежедневная проверка исполнителем наличия конфиденциальных материалов на рабочем месте. Состав проверяемых документов при квартальной проверке наличия документов. Процедура проверки правильности работы исполнителей с конфиденциальными документами. Состав проверяемых документов при годовой проверке наличия документов. Проверка наличия документов особой ценности. Основания и порядок проведения внеплановой проверки.

**РАЗДЕЛ V. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

**Тема 23. Технические меры защиты информации**

Понятие и виды технических мер обеспечения информационной безопасности и защиты информации. Виды угроз информационной безопасности, исходящих по техническим каналам. Анализ и оценка угроз информационной безопасности объекта, исходящих по техническим каналам. Средства и методы технической защиты объектов и информации. Правовое регулирование защиты информации с использованием технических средств. Регламентация использования технических средств защиты информации. Лицензирование помещений. Сертификация оборудования и технических средств защиты информации.

**Тема 24. Основы защиты информации в компьютерах, локальных сетях и средствах связи**

Состав информационных ресурсов в компьютерах, локальных сетях и средствах связи. Угрозы безопасности информации в процессе использования компьютеров, локальных сетей и средств связи. Организационные меры разграничения допуска и доступа к электронной информации. Технические средства пассивной и активной защиты электронной и цифровой информации. Программные средства защиты информационных ресурсов. Криптографическая защита информации. Защита информации в сети Интернет.

**4. ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ**

**Список источников и литературы[[1]](#footnote-1)**

Основной:

1. Банковский кодекс Республики Беларусь: [принят Палатой представителей 3 октября 2000 г.: одобрен Советом Республики 12 октября 2000 г.].
2. Бачило, И.Л. Информационное право / И.Л. Бачило. – СПб., 2013.
3. Введение в информационную безопасность: учебное пособие / Т. А. Пулко. – Минск : БГУИР, 2018.
4. Гражданский кодекс Республики Беларусь: [от 7 декабря 1998 г.].
5. Инструкция о порядке доступа к архивным документам, содержащим сведения, относящиеся к личной тайне граждан: утв. постановлением М-ва юстиции Респ. Беларусь, 24 мая 2012 г., № 132.
6. Инструкция о режиме доступа к документам, содержащим информацию, относящуюся к личной тайне граждан: утв. приказом Ком. по архивам и делопр. Респ. Беларусь, 3 июля 1996 г., № 21.
7. Инструкция по делопроизводству в государственных органах и организациях Республики Беларусь: утв. постановлением М– ва юстиции Респ. Беларусь, 19 янв. 2009 г., №4.
8. Информационная безопасность в системе СМИ: теоретико– правовой аспект / Н. Н. Довнар. – Минск : БГУ, 2013.
9. Информационная, психологическая и экологическая безопасность: учебно– методическое пособие по проведению кураторских и информационных часов / Н. В. Гапанович– Кайдалов, Е. В. Гапанович– Кайдалова. – Гомель : ГГТУ, 2014.
10. Информация и информационная безопасность. Правовой аспект / В.Г.Гавриленко. – Минск : Право и экономика, 2014.
11. Канстытуцыя Рэспублікі Беларусь = Конституция Республики Беларусь: [1994 года (са змяненнямі і дапаўненнямі): прынят. на рэспубліканскіх рэферэндумах 24 лістапада 1996 года і 17 кастрычніка 2004 года]. – Мінск: Беларусь, 2007.
12. Кибервойна: аспекты безопасности использования информационного пространства / Д. И. Вержбалович. – Минск : Беларуская Энцыклапедыя, 2015.
13. Кодекс Республики Беларусь об административных правонарушениях: Кодекс Респ. Беларусь, 21 апр. 2003 г., № 194– З: в ред. от 28 дек. 2009 г.
14. Концепция национальной безопасности Республики Беларусь: утверждена Указом Президента Республики Беларусь 9 ноября 2010 г. № 575.
15. Макаров, О.С. Актуальные аспекты обеспечения информационной безопасности государств-участников Содружества Независимых Государств: монография / О.С. Макаров. – Минск : ИНБ, 2013.
16. Национальная безопасность: информационно-психологическая безопасность, образование: монография / В. Ю. Арчаков и др. – Минск : ИПС Респ.Беларусь, 2018.
17. О государственных секретах: Закон Респ. Беларусь, 19 июля 2010 г.
18. О коммерческой тайне: Закон Респ. Беларусь, 5 янв. 2013 г., № 16-З.
19. О некоторых вопросах организации повышения квалификации, переподготовки, стажировки, организационного обучения, обучения в организации (по месту работы), постоянного профессионального совершенствования руководителей и специалистов в сфере защиты государ– ственных секретов: Постановление Совета Министров Респ. Беларусь, 2 окт. 2008 г., № 1445.
20. О некоторых мерах по упорядочению обращения с секретной документированной информацией Президента Республики Беларусь: Указ Президента Респ. Беларусь, 15 нояб. 2000 г., № 595: в ред. от 15 янв. 2009 г.
21. О регистре населения: Закон Респ. Беларусь, 21 июля 2008 г., № 418-З.
22. Об архивом деле и делопроизводстве в Республике Беларусь: Закон Респ. Беларусь, 25 нояб. 2011 г., № 323-З.
23. Об информации, информатизации и защите информации: Закон Респ. Беларусь, 10 но– яб. 2008 г., № 455– З.
24. Об определении перечня учреждений образования, обеспечивающих повышение квалификации, переподготовку и стажировку руководителей и специалистов, в компетенцию которых входит обеспечение защиты государственных секретов: постановление М-ва образ. Респ. Беларусь и К-та гос. безоп-ти Республики Беларусь, 28 нояб. 2008 г., № 119/67.
25. Распространение информации в интернете и СМИ: защита деловой репутации : [сборник статей]. – Минск : Информационное правовое агентство Гревцова, 2015.
26. Трудовой кодекс Республики Беларусь: [принят Палатой представителей 8 июня 1999 г.: одобрен Советом Республики 30 июня 1999 г.].
27. Уголовный кодекс Республики Беларусь: [принят Палатой представителей 2 июня 1999 г.: одобрен Советом Республики 24 июня 1999 г.].
28. Управление информационными ресурсами: материалы XV Международной научно-практической конференции (Минск, 7 декабря 2018 г.) / [редколлегия: Н. Л. Бондаренко, А. И. Ящук, Б. В. Новыш]. – Минск : Академия управления при Президенте Республики Беларусь, 2018.

Дополнительный:

1. Буч, Ю.И. Охрана ноу-хау / Ю.И. Буч, М.А. Колесникова. – СПб., 1995.
2. Венгеров, А.Б. Право и информация в условиях автоматизации управления (теоретические вопросы) / А.Б. Венгеров – М.: Юрид. лит.,1978.
3. Вирковский, В.А. Некоторые вопросы защиты государственной тайны в ходе научных исследований / В.А. Вирковский // Вопросы защиты информации. – 1998. – № 1–2.
4. Вус, М.А. Информационно-коммерческая безопасность. Защита коммерческой тайны / М.А. Вус, В.П. Морозов. – СПб.: Дом коммерч. бумаг, 1993.
5. Гаврилов, Э. К вопросу об охране коммерческой, служебной и личной тайны. Гражданско-правовые аспекты / Э. Гаврилов //Хозяйство и право. – 2003. – №5 .
6. Гасанов, P.M. Шпионаж и бизнес / Р.М. Гасанов. – М., 1992.
7. Демушкин, А.С. Документы и тайна / А.С. Демушкин. – М., 2003.
8. Доронин, А.И. Бизнес-разведка / А.И. Доронин. – М., 2002.
9. Драчёв, С.С. Основы корпоративной безопасности / С.С. Драчёв. – СПб., 2000.
10. Землянов, В.М. Своя контрразведка / В.М. Землянов. – Минск, 2002.
11. Информационно-коммерческая безопасность. Защита коммерческой тайны: пособие. – М., 1993.
12. Информационные технологии и безопасность. Криптология. Термины и определения: СТБ 34.101.69– 2014. – Минск : Госстандарт, Белорусский государственный институт стандартизации и сертификации, 2014.
13. Информационные технологии и безопасность. Синтаксис криптографических сообщений: СТБ 34.101.23– 2012. – Минск : Госстандарт, Белорусский государственный институт стандартизации и сертификации, 2012. – IV, 34 с.
14. Информационные технологии. Средства защиты информации. Информационная безопасность: ТР 2013/027/BY: [утверждено Советом Министров Республики Беларусь 15.05.2013: введено 01.01.2014]. – Изд. официальное. – Минск : Госстандарт, Белорусский государственный институт стандартизации и сертификации, 2013.
15. Коммерческая тайна предприятия / А.Н. Трунов. – М., 1993.
16. Копылов, В.А. Информационное право: учебник / В.А. Копылов. – М.: Юристъ, 2005.
17. Кузнецов, И.Н. Информация: сбор, защита, анализ / И.Н.Кузнецов – Минск, 2002.
18. Кураков, Л.П. Информация как объект правовой защиты / Л.П.Кураков, С.Н. Смирнов. – М.: Гелиос, 1998.
19. Курушев, В.Д. Компьютерные преступления и информационная безопасность / В.Д. Курушев, В.А. Минаев. – М.: Новый юрист, 1998.
20. Лукашов, А.И. Конфиденциальная информация и коммерческая тайна: правовое регулирование и организация защиты / А.И. Лукашов, Г.Н.Мухин. – Минск: Тесей, 1998.
21. Мазуров, В.А. Тайна государственная, коммерческая, банковская, частной жизни. Уголовно-правовая защита / В.А. Мазуров. – М., 2003.
22. Мак-Мак, В.П. Служба безопасности предприятия. Организационно-управленческие и правовые аспекты деятельности / В.П.Мак-Мак. – М.: Мир безопасности, 1999.
23. Международный конгресс по информатике: информационные системы и технологии [Электронный ресурс]: материалы международного научного конгресса, Республика Беларусь, 24―27 октября 2016 г. / редколлегия: С. В. Абламейко (главный редактор) [и др.]. – Минск : БГУ, 2016. – 1 электронный оптический диск (CD– ROM).
24. Методика информационной безопасности / Ю.С. Уфимцев [и др.]. – М.: Изд-во «Экзамен», 2004.
25. Овчинский, С.С. Оперативно-розыскная информация / С.С.Овчинский. М., 2000.
26. Организация и современные методы защиты информации / Под ред. С.И. Диева, А.Г. Шаваева. – М., 1998.
27. Панченко, П.Н. Институт тайны: правоохранительные аспекты / П.Н. Панченко // Государство и право. – 1998. – № 8.
28. Петраков, А.В. Защита и охрана личности, собственности, информации / А.В. Петраков. – М., 1997.
29. Петрухин, И.Л. Личные тайны (человек и власть) / И.Л. Петрухин. – М., 1998.
30. Преступления в информационной сфере: проблемы расследования, квалификации, реализации ответственности и предупреждения: материалы Международной научно– практической конференции, 14―15 февраля 2013 года / [редколлегия: В. А. Шуняева, Е. А. Попова, С. А. Пучнина]. – Тамбов : Издательство ТГУ, 2013. – 284 с.
31. Рассолов, М.М. Информационное право: учеб. пособие / М.М. Рассолов. – М.: Юристъ, 1999.
32. Северин, В.А. Правовое обеспечение информационной безопасности предприятия / В.А. Северин. – М., 2000.
33. Соловьёв, Э. Коммерческая тайна и её защита / Э. Соловьёв. – М., 2001.
34. Степанов, Е.А. Информационная безопасность и защита информации: учеб. пособие / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2001.
35. Технические средства защиты информации: тезисы докладов XV Белорусско-российской научно-технической конференции (Минск, 6 июня 2017 года) / [редколлегия: Т. В. Борботько и др.]. – Минск : БГУИР, 2017.
36. Фатьянов, А.А. Тайна и право (основные системы ограничений на доступ к информации в российском праве) / А.А. Фатьянов. – М., 1998.
37. Халяпин, Д.Б. Основы защиты информации: учеб. пособие / Д.Б.Халяпин, В.И. Ярочкин. – М.: ИПКИР, 1994.
38. Шаваев, А.Г. Безопасность корпораций. Криминологические, уголовно-правовые и организационные проблемы / А.Г. Шаваев. – М.: Концерн «Банковский деловой центр», 1998.
39. Шиверский, А.А. Защита информации: проблемы теории и практики / А.А. Шиверский. – М.: Юристъ, 1996.
40. Ярочкин, В.И. Информационная безопасность: учебник для вузов / В.И. Ярочкин. – М., 2000.
41. Ярочкин, В.И. Служба безопасности коммерческого предприятия. Организационные вопросы / В.И. Ярочкин. – М., 1995.

**Методические рекомендации по организации и выполнению самостоятельной работы обучающихся по учебной дисциплине**

Самостоятельная работа студентов играет важную роль в изучении дисциплины. Самостоятельная работа предусматривает выполнение тестов, сдачу промежуточных зачетов, выполнение учебно-исследовательских заданий разного уровня сложности, ознакомление с учебной, учебно-методической и научной литературой, нормативными правовыми актами, техническими нормативными правовыми актами.

Среди рекомендуемых видов занятий необходимо отдельно выделить составление и решение практикоориентированных задач, реферирование и рецензирование специальных трудов, работу с правовыми источниками.

В числе педагогических методик и технологий преподавания дисциплины, способствующих вовлечению студентов в поиск и управление знаниями, приобретению опыта самостоятельного решения задач и инновационной деятельности, следует выделить: технологии модульного, проектного обучения, деловые игры, лекции-конференции/дискуссии и технологии учебно-исследовательской и эвристической деятельности.

**Перечень рекомендуемых средств диагностики**

Основным средством диагностики усвоения знаний и овладения необходимыми умениями и навыками по дисциплине «Информационная безопасность и защита информации» является проверка заданий разнообразного типа (репродуктивных, реконструктивных, вариативных), выполняемых в рамках часов, отводимых на семинарские занятия, контрольные работы, компьютерное тестирование.

Для диагностики могут использоваться консультация, собеседование, письменная работа (реферат, эссе), фронтальный опрос на лекциях и другие формы контроля.

Текущий и заключительный контроль по дисциплине осуществляются с использованием организационных форм и количественных показателей контроля, закрепленных в соответствии с действующей системой оценки успеваемости студентов.

1. Тексты правовых актов Республики Беларусь приведены по информационной системе «Консультант Плюс: Беларусь. Технология ПРОФ» [Электронный ресурс] / ООО “ЮрСпектр”, Нац. центр правовой информации Респ. Беларусь. – Минск, 2018. [↑](#footnote-ref-1)