

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Проректор по науке
и международным связям

А.В. Толстиков

2 марта 2020 г.



ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рабочая программа

для обучающихся по направлению подготовки

10.06.01 Информационная безопасность

Профиль (направленность):

Методы и системы защиты информации, информационная безопасность
форма обучения (очная)

Захаров А.А. Защита информационных систем персональных данных. Рабочая программа для обучающихся по направлению подготовки 10.06.01 Информационная безопасность, профиль (направленность): методы и системы защиты информации, информационная безопасность, форма обучения (очная). Тюмень, 2020.

Рабочая программа дисциплины (модуля) Защита информационных систем персональных данных опубликована на сайте ТюмГУ: [электронный ресурс] / Режим доступа: <https://www.utmn.ru/sveden/education/#>

1. Пояснительная записка.

Целью изучения дисциплины «Защита информационных систем персональных данных» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой персональных данных, обучением принципам и методам защиты информации в информационных системах персональных данных (ИСПДн).

Задачи дисциплины:

- изучение типовых угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
- овладение средствами и методами проектирования и построения защищенных ИСПДн;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности ИСПДн.

1.1. Место дисциплины в структуре образовательной программы (ОП):

Данная дисциплина входит в Б1 Блок 1 «Дисциплины (модули)» Вариативная часть (обязательные дисциплины).

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины

Код и наименование компетенции	Компонент (знаниевый/функциональный)
ПК-4 - способность к созданию новых и совершенствованию существующих средств защиты информации, циркулирующей в системах документооборота (вне зависимости от степени их компьютеризации).	Знает: -основные понятия теории защиты информации. Умеет: -обнаруживать и ставить задачи, содержащие необходимость использования средств защиты информации.
ПК-6 - способность к созданию новых и совершенствованию существующих моделей и методов формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.	Знает: -возможности существующих моделей и методов формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации Умеет: -создавать новые и совершенствовать существующие средства противодействия нарушению информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования
ПК-9 - способность к созданию новых и совершенствованию существующих моделей и методов оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты вне	Знает: -основы обеспечения информационной безопасности объектов защиты вне зависимости от области их функционирования. Умеет:

1	2	3	4	5	6	7
1.	Требования Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» к обеспечению безопасности персональных данных, обрабатываемых и хранящихся в ИСПДн	24	4	4	0	0
2.	Классификация ИСПДн. Постановление Правительства № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	24	4	4	0	0
3.	Модель угроз персональных данных (ПД). Сетевые атаки. Модель злоумышленника	24	4	4	0	0
4.	Организация и обеспечение режимов защиты персональных данных	24	4	4	0	0
5.	Программно-аппаратные средства защиты информации, применяемые при защите информационных систем персональных данных	24	4	4	0	0
6.	Криптографические средства защиты информации, применяемые при защите информационных систем персональных данных	22	4	4	0	0
7.	Зачет	2	0	0	0	2
	Итого (часов)	144	24	24	0	2

4.2. Содержание дисциплины по темам

Тема 1. Требования Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» к обеспечению безопасности персональных данных, обрабатываемых и хранящихся в ИСПДн.

Основные понятия. Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации. Содержание категории «персональные данные». Область применения закона. Ограничения.

Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение.

Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта. Обработка биометрических данных. Обработка персональных данных третьим лицом в интересах оператора. Трансграничная передача персональных данных. Специальные категории персональных данных и особенности их обработки. Права субъектов персональных данных и их соблюдение при обработке. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.

Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными.

Тема 2. Классификация ИСПДн. Постановление Правительства Российской

Федерации от 1 ноября 2012 г. № 1119 г. Москва «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Порядок проведения классификации информационных систем персональных данных.

Руководящие документы ФСТЭК и ФСБ России по защите персональных данных. Нормативно-методическое обеспечение безопасности информационных систем персональных данных в органах власти, учреждениях (предприятиях).

Порядок лицензирования операторов информационных систем персональных данных.

Мероприятия по защите сведений конфиденциального характера, основные внутренние нормативные документы, меры по охране конфиденциальности; формирование перечня персональных данных.

Ограничение доступа к персональным данным, учет лиц, допущенных к персональным данным, определение порядка обращения с такими сведениями, контроля над его соблюдением, организация доступа к персональным данным, внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие, контроль над соблюдением режима конфиденциальности.

Тема 3. Модель угроз персональных данных (ПД). Сетевые атаки. Модель злоумышленника.

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Модель сетевых угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Модель злоумышленника информационных систем персональных данных.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.

Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных различных классов.

Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации.

Требования к подготовке к утилизации и порядок утилизации персональных данных и машиночитаемых носителей информации, используемых в обработке персональных данных.

Тема 4. Организация и обеспечение режимов защиты персональных данных.

Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных. Защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.

Необходимость обработки персональных данных. Перечень персональных данных, подлежащих защите от несанкционированного доступа. Условия расположения информационных систем обработки персональных данных относительно границ контролируемой зоны. Конфигурация и топология информационных систем персональных данных. Степень участия персонала. Угрозы безопасности персональных данных.

Этапы и порядок внедрения средств обеспечения информационной безопасности информационных систем персональных данных.

Мероприятия по контролю обеспечения безопасности персональных данных. Механизмы и средства контроля. Периодичность и содержание работ. Ответственность оператора за нарушение правил обращения с персональными данными. Подготовка уведомлений об обработке персональных данных в уполномоченный орган.

Тема 5. Программно-аппаратные средства защиты информации, применяемые при защите информационных системах персональных данных.

Современные программно-аппаратные средства. Возможности и основы применения средств защиты информации от несанкционированного доступа, средств антивирусной защиты, средств сетевой защиты.

Обоснование разработки системы защиты персональных данных. Исходные данные создаваемой (модернизируемой) информационной системы в техническом, программном, информационном и организационном аспектах. Разработка собственных средств защиты информации. Состав, содержание и сроки проведения работ по этапам разработки и внедрения системы защиты персональных данных. Контроль и надзор за эксплуатацией аттестованных информационных систем персональных данных. Порядок обслуживания и ремонта аттестованных информационных систем. Ответственность лиц.

Условия расположения информационных систем обработки персональных данных относительно границ контролируемой зоны. Конфигурация и топология информационных систем. Степень участия персонала.

Тема 6. Криптографические средства защиты информации, применяемые при защите информационных системах персональных данных.

Симметричные и ассиметричные криптосистемы. Проблемы факторизации и дискретного логарифмирования. Криптография на эллиптической кривой.

Криптографические протоколы. Схема разделения секрета. Применение криптографических средств в информационных системах персональных данных.

Современные криптографические средства защиты информации. Возможности и применение шифровальных средств и средств электронно-цифровой подписи (ЭЦП).

Инфраструктура открытых ключей. Сертификат открытого ключа.

Защищенный электронный документооборот персональных данных. Использование электронной цифровой подписи в информационных системах персональных данных.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№	Темы	Виды СРА		Объем часов
		обязательные	дополнительные	
1	Требования Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» к обеспечению безопасности персональных данных, обрабатываемых и хранящихся в ИСПДн.	Конспектирование материала на лекционных занятиях. Выполнение практических заданий.	Работа с литературой. Работа с программными средствами.	16

Примерные темы рефератов:

1. Разработка модели угроз для информационной системы персональных данных;
2. Разработка политики безопасности для информационной системы персональных данных;
3. Определение уровня защищённости для информационной системы персональных данных;
4. Определение класса государственных информационных систем;
5. Построение и анализ графа атак для информационной системы персональных данных;
6. Обезличивание персональных данных в информационных системах персональных данных.

Вопросы к зачёту:

- 1) Определение персональных данных (ПДн) и информационной системы персональных данных.
- 2) Нормативно-правовая база в сфере защиты и обработки ПДн (№ 149-ФЗ, № 152-ФЗ).
- 3) Категории персональных данных.
- 4) Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении
- 5) требований к защите персональных данных при их обработке в информационных системах персональных данных».
- 6) Уровни защищённости информационных систем персональных данных.
- 7) Процесс подготовки пакета документов к аккредитации ИСПДн: обязательство о неразглашении информации, содержащей ПДн; согласие на обработку ПДн; перечень ИСПДн.
- 8) Процесс подготовки пакета документов к аккредитации ИСПДн: перечень ПДн, обрабатываемых и хранящихся в ИСПДн; положение об обработке ПДн работников; акт определения уровня защищённости ИСПДн.
- 9) Принципы обеспечения безопасности ПДн.
- 10) Обезличивание ПДн. Абсолютное обезличивание и относительное обезличивание.
- 11) Нормативно-правовая база в области обезличивания ПДн (Приказ Роскомнадзора от 5 сентября 2013 г. №996 «Об утверждении требований и методов по обезличиванию ПДн»).
- 12) Свойства обезличенных данных. Свойства методов обезличивания.
- 13) Методы обезличивания персональных данных. Сравнительный анализ методов обезличивания.
- 14) Алгоритм перемешивания данных в общем виде.
- 15) Формальное описание алгоритма обезличивания ПДн методом перемешивания с помощью циклических перестановок.
- 16) Анализ эффективности алгоритма перемешивания ПДн с помощью циклических перестановок.
- 17) Определение политик безопасности (ПБ). Представление ПБ.
- 18) Закрытые, открытые, гибридные политики информационной безопасности.
- 19) Методы описания ПБ. Сравнительный анализ методов описания ПБ.
- 20) Аналитический метод описания ПБ.
- 21) Графовый метод описания ПБ.
- 22) Объектный метод описания ПБ.
- 23) Логический метод описания ПБ.
- 24) Пример графового метода описания ПБ: визуальный язык объектных ограничений «Language on Objects for Security Constraints» (LaSCO).

2.	ПК-6 - способность к созданию новых и совершенствованию существующих моделей и методов формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования	Знает: -возможности существующих моделей и методов формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации Умеет: -создавать новые новых и совершенствовать существующие средства противодействия нарушению информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования	Вопросы по реферату и зачету	примеры, иллюстрирующие излагаемый теоретический материал. Во всех остальных случаях аспирант получает отметку «незачтено»
3.	ПК-9 - способность к созданию новых и совершенствованию существующих моделей и методов оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты вне зависимости от области их функционирования	Знает: -основы обеспечения информационной безопасности объектов защиты вне зависимости от области их функционирования. Умеет: -обнаруживать и ставить задачи, содержащие необходимость использования средств защиты информации. Знает: -существующие технологии идентификации и аутентификации пользователей. Умеет: -целесообразно применять существующие технологии идентификации и аутентификации пользователей в ИСПДн.	Вопросы по реферату и зачету	

4.	ПК-10 Способность к созданию новых и совершенствованию существующих технологий идентификации и аутентификации пользователей и субъектов информационных процессов.	Знает: -основные понятия теории защиты информации. Умеет: -обнаруживать и ставить задачи, содержащие необходимость использования средств защиты информации.	Вопросы по реферату и зачету	
----	---	---	------------------------------	--

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Криптография и безопасность цифровых систем: Учебное пособие / Грибунин В.Г., Мартынов А.П., Николаев Д.Б. - Саратов:ФГУП"РФЯЦ-ВНИИЭФ", . - 411 с.: ISBN. - Текст : электронный. - URL: <https://znanium.com/catalog/product/950489> (дата обращения: 01.03.2020). – Режим доступа: по подписке.

2. Петренко, С. А. Политики безопасности компании при работе в Интернет / Петренко С.А., Курбатов В.А., - 3-е изд., (эл.) - Москва :ДМК Пресс, 2018. - 397 с.: ISBN 978-5-93700-057-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/983161> (дата обращения: 01.03.2020). – Режим доступа: по подписке.

7.2. Дополнительная литература:

1. Олифер, В. Г. Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва : ИНТУИТ, 2016. — 219 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/100346> (дата обращения: 01.03.2020). — Режим доступа: для авториз. пользователей.

2. Построение коммутируемых компьютерных сетей : учебное пособие / Е. В. Смирнова, И. В. Баскаков, А. В. Пролетарский, Р. А. Федотов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 428 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/100370> (дата обращения: 01.03.2020). — Режим доступа: для авториз. пользователей.

7.3. Интернет-ресурсы

1. Интернет ресурсы Academy Cisco <http://netacad.com>

7.4. Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) <https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true>
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) <https://icdlib.nspu.ru/>
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА <https://rusneb.ru/>
- Справочная правовая система КонсультантПлюс <http://www.consultant.ru/>

Наименование ПО

- Microsoft Office 365

- "Microsoft Imagine Academy (панель Dreamspark):MS Visual Studio, MS SQL Server, ОС семейства MS Windows, MS Visio, MS Project"

7.5. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- эмулятор сетей PacketTracer. версия 7.x;
- эмулятор сетей GNS3 2.*
- эмулятор сетей eNSP 1.3.*
- гипервизор Oracle Virtual Box 5.*
- платформа для электронного обучения Microsoft Teams

Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной системы.

7.6. Источники Интернет:

1. ФСБ России [Электронный ресурс]. – Режим доступа: <http://fsb.ru> (дата обращения 01.02.2020);
2. ФСТЭК России [Электронный ресурс]. – Режим доступа: <http://fstec.ru> (дата обращения 01.02.2020).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

- Свободно распространяемая система виртуализации Virtual Box;
- Операционная система Linux;
- Свободно распространяемый прокси-сервер SQUID;
- Свободно распространяемое программное обеспечение для организации виртуальных частных сетей OpenVPN;
- Свободно распространяемая система обнаружения вторжений Snort;
- Свободно распространяемый сервер удалённого доступа OpenSSH.

9. Технические средства и материально-техническое обеспечение дисциплины.

Для практических занятий необходимо наличие компьютерного класса, объединенного в локальную вычислительную сеть. На компьютерах должны быть установлены серверные версии операционной системы (ОС) Linux (в качестве альтернативы предусматривается развертывание ОС в рамках виртуальных машин). В качестве коммуникационного оборудования могут использоваться коммутаторы, позволяющие организовать VLAN. Желательно наличие маршрутизатора, а также доступа в глобальную вычислительную сеть Интернет. В целях сохранения результатов работы желательно, чтобы аспиранты имели при себе носители информации (flash-накопители).