*Общество с ограниченной ответственностью «Развитие плюс»*
*630001, г.Новосибирск, ул.Сухарная, дом 15а, оф.7,*
*тел. (383)373-96-26 e-mail: grazvitie@inbox.ru*
*ИНН 5402030244 КПП 540201001 ОГРН 1175476034777*

**УТВЕРЖДЕНО**
**приказом Директора ЦПКиПП «Развитие плюс»**
**О.В. Дворядкиной**
**от «01» января 2020 № 005**

# РАБОЧАЯ ПРОГРАММА

учебной дисциплины ««**Защита персональных данных в РФ. Проблемы по внесению и обработке персональных данных на общероссийский сайтах (bus.gov.ru) в 2020 г.» (72 ак.ч.)**

Разработчик: Павленко Е.Ю., преподаватель ЦПКиПП ООО «Развитие плюс»

Рабочая программа учебной дисциплины рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии общепрофессиональных дисциплин от «01» января 2020 года

**Новосибирск 2020**

Общество с ограниченной ответственностью «Развитие плюс»
630001, г.Новосибирск, ул.Сухарная, дом 15а, оф.7,
тел. (383)373-96-26 e-mail: grazvitie@inbox.ru
ИНН 5402030244 КПП 540201001 ОГРН 1175476034777

## 1. Пояснительная записка

### 1.1. Цели и задачи дисциплины

Учебная дисциплина «Защита персональных данных» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

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

**Задачи** дисциплины «Защита персональных данных»:

• 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.

### 1.2. Место дисциплины в структуре образовательной программы

В результате изучения этих дисциплин студент

должен ***знать***:

•подходы к правовой защите информации, к организации контроля над возможными каналами их утечки;

- методы и способы выявления угроз безопасности данных при их обработке в информационных системах;
- порядок организации работ по обеспечению безопасности информации в информационных системах;
- основные технические, программные, криптографические, программно-аппаратные средства, применяемые для защиты данных;
- методы контроля и оценки состояния обеспечения безопасности данных в информационных системах;

***уметь***:

- разрабатывать модели угроз для информационных систем с учетом их назначения, условий и особенностей функционирования;
- разрабатывать необходимую организационно-распорядительную и нормативно-техническую документацию в интересах системы защиты информационных систем;
- оценивать эффективность системы защиты информационных систем.

### 1.3. Компетенции обучающегося, формируемые в результате освоения данной образовательной программы.

В результате освоения ОП Слушатель должен обладать следующими компетенциями:

***профессиональными (ПК):***

- способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);
- способностью организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности (ПК-30);

Общество с ограниченной ответственностью «Развитие плюс»
630001, г.Новосибирск, ул.Сухарная, дом 15а, оф.7,
тел. (383)373-96-26 e-mail: grazvitie@inbox.ru
ИНН 5402030244 КПП 540201001 ОГРН 1175476034777

- способностью использовать нормативные правовые акты в своей профессиональной деятельности (ПК- 6).

**1.4. Перечень планируемых результатов обучения по дисциплине (модулю):**

***знать***:

- основные особенности современного состояния организационно-правового обеспечения защиты персональных данных в информационных системах персональных данных;
- проблемы охраны конфиденциальности персональных данных лиц в Российской Федерации;
- требования и рекомендации по обеспечению безопасности информации в информационных системах персональных данных;

***уметь***:

- составлять перечень сведений, отнесенных к персональным данным, и проводить их классификацию;
- проводить классификацию информационных систем персональных данных с составлением соответствующего акта;
- выявлять актуальные угрозы безопасности информации в информационных системах персональных данных;
- планировать, организовывать и контролировать выполнение работ и мероприятий по защите персональных данных;

***владеть:***

- навыками применения программно-аппаратных средств защиты персональных данных;
- навыками разработки внутренних нормативных документов, обеспечивающих защиту персональных данных в информационных системах персональных данных.

Общество с ограниченной ответственностью «Развитие плюс»
630001, г.Новосибирск, ул.Сухарная, дом 15а, оф.7,
тел. (383)373-96-26 e-mail: grazvitie@inbox.ru
ИНН 5402030244 КПП 540201001 ОГРН 1175476034777

## 2. Структура и трудоемкость дисциплины.

Форма промежуточной аттестации – зачѐт. Общая трудоемкость дисциплины составляет 72 академических часа.

## 3. Тематический план (Учебный план)

| п/н | Модули обучения | лекции | Самостоят. работа |
|---|---|---|---|
| **1.** | **Защита персональных данных в РФ в соответствии с нормами Федерального закона № 152-ФЗ «О защите персональных данных» от 27.07.2006 года (с изменениями 2020)** | **13** | **5** |
| 1.1 | Что такое персональные данные? | 3 | 1 |
| 1.2. | Что такое субъект и оператор персональных данных? | 3 | 1 |
| 1.3 | Как классифицировать информационную систему персональных данных? | 2 | |
| 1.4 | Порядок действий по защите информационной системы персональных данных. | 2 | 1 |
| 1.5. | Когда аттестация и сертификация обязательны? | 3 | 2 |
| **2.** | **Ответственность за нарушения по обработке персональных данных.** | **9** | **3** |
| 2.1. | Какие персональные данные можно обрабатывать без уведомления. | 1 | 1 |
| 2.2. | Виды проверок Роскомнадзора. | 1 | 1 |
| 2.3. | Как выполнить требования законодательства и подготовиться к проверке Роскомнадзора. | 2 | |
| 2.4. | Если же вы решили действовать самостоятельно….. | 5 | 1 |
| 2.4. 1. | 5 базовых принципов Закона о защите персональных данных, которые нужно знать. | 2 | |
| 2.4. 2. | Правовые, Организационные, Технические меры реализации норм закона. | 2 | |
| 2.4. 3. | Работа на Общероссийских сайтахZakupki.gov.ru; Torgi.gov.ru; Bus.gov.ru | 1 | 1 |
| 2.4. 4. | Варианты решений руководителя. | 1 | |
| **3.** | **Надзор и контроль в сфере обработки персональных данных.** | **15** | **5** |
| 3.1. | Надзор и контроль в сфере обработки персональных данных на примере Краснодарского края и Республики Адыгея. | 2 | |
| 3.2. | Последние новости по проверкам применения норм Федерального закона № 152-ФЗ «О защите персональных данных» в Республике Крым и г. Севастополь! | 5 | |
| 3.3. | Типовые документы, формы и образцы их заполнения… | 3 | 5 |
| 3.3. 1. | Форма уведомления. | | |
| 3.3. 2. | Образец Заполнения уведомления. | | |
| 3.3. 3. | Рекомендации по заполнению уведомления. | | |
| 3.3. 4. | Информационное письмо о внесении изменений в сведения об операторе в реестре операторов, осуществляющих обработку персональных данных. | | |
| 3.3.5. | Заявление об исключении сведений об операторе из реестра операторов, осуществляющих обработку персональных данных. | | |

Общество с ограниченной ответственностью «Развитие плюс»
630001, г.Новосибирск, ул.Сухарная, дом 15а, оф.7,
тел. (383)373-96-26 e-mail: grazvitie@inbox.ru
ИНН 5402030244 КПП 540201001 ОГРН 1175476034777

| | | | |
|---|---|---|---|
| 3.3.6. | Заявление о предоставлении выписки из | | |
| **4.** | **Подзаконные акты, используемые при проверках.** | **17** | |
| 4.1. | Постановление от 3 ноября 1994г. №1233 Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в Федеральных органах исполнительной власти. | 2 | |
| 4.2. | Постановление от 6 июля 2008 г. № 512 Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. | 3 | |
| 4.3. | Постановление от 15 сентября 2008г. №687 Об утверждении положения об особенностях обработки персональных данных, осуществляемой использования средств автоматизации. | 2 | |
| 4.4. | Приказ от 15 марта 2013 г. N 274 об утверждении перечня иностранных государств, не являющихся сторонами конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. | 2 | |
| 4.5. | Приказ от 21 декабря 2011 г. N 346 об утверждении административного регламента федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги "ведение реестра операторов, осуществляющих обработку персональных данных". | 3 | |
| 4.6. | Постановление от 21 марта 2012 г. N 211 Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами. | 1 | |
| 4.7. | Постановление от 1 ноября 2012 г. N 1119 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных. | 1 | |

Общество с ограниченной ответственностью «Развитие плюс»
630001, г.Новосибирск, ул.Сухарная, дом 15а, оф.7,
тел. (383)373-96-26 e-mail: grazvitie@inbox.ru
ИНН 5402030244 КПП 540201001 ОГРН 1175476034777

| | | | |
|---|---|---|---|
| 4.8. | Приказ от 14 ноября 2011 г. N 312 об утверждении административного регламента исполнения федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства российской федерации в области персональных данных. | 1 | |
| 5 | Итоговое тестирование | | 5 |
| | Итого | **54** | **18** |
| | Общее количество | **72** | |

Общество с ограниченной ответственностью «Развитие плюс»
630001, г.Новосибирск, ул.Сухарная, дом 15а, оф.7,
тел. (383)373-96-26 e-mail: grazvitie@inbox.ru
ИНН 5402030244 КПП 540201001 ОГРН 1175476034777

**4. Содержание дисциплин.**

1. **Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации.** Основные понятия и определения. Содержание категории «персональные данные». Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение.

2. **Принципы обработки персональных данных.** Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта. Обработка биометрических данных. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными. Специальные категории персональных данных и особенности их обработки. Права субъектов персональных данных и их соблюдение при обработке.

3. **Трансграничная передача персональных данных.** Обработка персональных данных третьим лицом в интересах оператора. 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. Ответственность за нарушение требований по обращению с персональными данными.

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

5. **Нормативно-методическое обеспечение безопасности 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.

6. **Классификация информационных систем персональных данных.** 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». Порядок проведения классификации информационных систем персональных данных.

7. **Модель угроз для информационных систем персональных данных.** Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Модель злоумышленника информационных систем персональных данных. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.

8. **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.

9. **Оценка эффективности систем защиты информационных систем персональных данных.** Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных

Общество с ограниченной ответственностью «Развитие плюс»
630001, г.Новосибирск, ул.Сухарная, дом 15а, оф.7,
тел. (383)373-96-26 e-mail: grazvitie@inbox.ru
ИНН 5402030244 КПП 540201001 ОГРН 1175476034777

системах персональных данных требованиям безопасности информации. 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.

**5. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующей этапы формирования компетенций в процессе освоения образовательной программы.**

**Примерные темы контрольных работ:**

1. Уровни защищѐнности информационных систем персональных данных;
2. Классы защищѐнности государственных информационных систем;
3. Обезличивание персональных данных;
4. Описание политики безопасности с помощью аналитического метода;
5. Описание политики безопасности с помощью графового метода;
6. Описание политики безопасности с помощью объектного метода;
7. Описание политики безопасности с помощью логического метода;
8. Анализ графа атак;
9. Построение гарантированной (верифицируемой) защиты;
10. Вероятностная оценка реализации канала НСДУВ.

**Вопросы к зачѐту:**

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 требований к защите персональных данных при их обработке в информационных системах персональных данных».

5) Уровни защищѐнности информационных систем персональных данных.

6) Процесс подготовки пакета документов к аккредитации ИСПДн: обязательство о неразглашении информации, содержащей ПДн; согласие на обработку ПДн; перечень ИСПДн.

7) Процесс подготовки пакета документов к аккредитации ИСПДн: перечень ПДн, обрабатываемых и хранящихся в ИСПДн; положение об обработки ПДн работников; акт определения уровня защищѐнности ИСПДн.

8) Принципы обеспечения безопасности ПДн.

9) Обезличивание ПДн. Абсолютное обезличивание и относительное обезличивание.

10) Нормативно-правовая база в области обезличивания ПДн (Приказ Роскомнадзора от 5 сентября 2013 г. №996 «Об утверждении требований и методов по обезличиванию ПДн»).

11) Свойства обезличенных данных.

12) 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.

Общество с ограниченной ответственностью «Развитие плюс»
630001, г.Новосибирск, ул.Сухарная, дом 15а, оф.7,
тел. (383)373-96-26 e-mail: grazvitie@inbox.ru
ИНН 5402030244 КПП 540201001 ОГРН 1175476034777

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).
25) Определение графа атак. Формальное описание построения модели графа атак.
26) Анализ графа атак. Модель злоумышленника.
27) Определение гарантированной (верифицируемой) защиты.
28) Методы обеспечения гарантированности защиты.
29) Каналы несанкционированного доступа, утечки информации и деструктивных воздействий на информационную среду (НСДУВ).
30) Вероятностная оценка реализации канала НСДУВ.

**10.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности характеризующих этапы формирования компетенций.**

К зачѐту допускаются студенты, набравшие за семестр 35 баллов. Зачѐт проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения зачѐта студентом должно быть сдано минимум 5 лабораторных работ и сделаны ответы на 2 вопроса из билета. Ответы должны быть подробными, в полной мере раскрывать тему и не содержать грубых или существенных ошибок.

**11. Образовательные технологии.**

В учебном процессе используются традиционные виды учебной активности – лекционные и лабораторные занятия. Также применяются активные и интерактивные виды учебной активности, например, совместное обсуждение материала, круглые столы по вопросам участия в научных конференциях по теме предмета; обсуждение материалов конференций и статей в последних научных журналах, широко освещающих тематику информационной безопасности, например, «Information Security», выполнение студентами под руководством преподавателя обзоров отечественной и зарубежной литературы по заданной теме.

**12. Учебно-методическое и информационное обеспечение дисциплины.**

**12.1. Основная литература:**

1. Башлы, П.Н. Информационная безопасность и защита информации: Учебник [Электронный ресурс] / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – М.: РИОР, 2013. – 222 с. – Режим доступа: http://znanium.com/bookread.php?book=405000 (дата обращения 01.02.2015);
2. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие [электронный ресурс] / В.Ф. Шаньгин. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. – 592 с. – Режим доступа: http://znanium.com/bookread.php?book=402686 (дата обращения 01.02.2015).

**12.2. Дополнительная литература:**

3. Бабаш, А.В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. – 2-е изд. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. – 216 с. – Режим доступа: http://znanium.com/bookread.php?book=432654 (дата обращения 01.02.2015);
4. Дубинин, Е.А. Оценка относительного ущерба безопасности информационной системы: Монография [электронный ресурс] / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. – 192 с. – Режим доступа: http://znanium.com/bookread.php?book=471787 (дата обращения 01.02.2015);