Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет

информатики и радиоэлектроники»

Факультет радиотехники и электроники

Кафедра информационных радиотехнологий

Дисциплина: Методика преподавания общетехнических

и специальных дисциплин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовой работе

на тему

**методическая разработка раздела "Организация   
тестирования программного обеспечения" по   
дисциплине "Тестирование и отладка программного обеспечения" уровня среднего специального   
образования**

БГУИР КР 1-08 01 01-07 13 ПЗ

Студент: гр. 844691 Новосёлов Н.А.

Руководитель: кандидат педагогических наук, доцент Парафиянович Т.А.

Минск 2020

**Реферат**

методическая разработка раздела «Организация тестирования программного обеспечения» по дисциплине «Тестирование и отладка программного обеспечения» уровня среднего специального образования: курсовая работа / В.А.Сабило. – Минск: БГУИР, 2020, п.з. – 89 с., CD-R – 1 шт.

В настоящем времени актуален вопрос о методике преподавания общетехнических и специальных дисциплин. Образование нуждается в улучшении существующих методик, а также в создании новых. Это способствует улучшению качества и процесса обучения.

Объектом исследования является образовательный процесс уровня среднего специального образования, предметом исследования — методика преподавания дисциплины «Тестирование и отладка программного обеспечения».

Цель исследования — обоснование и разработка элементов содержания обучения и методики преподавания по дисциплине «Тестирование и отладка программного обеспечения» уровня среднего специального образования.

Перед курсовой работой были поставлены следующие задачи:

1. Выявить и описать основные характеристики образовательного процесса уровня среднего специального образования и используемой дидактической системы;

2. Выявить на основе анализа типовой учебной программы, частных методик, спрогнозировать и описать особенности методики преподавания дисциплины «Тестирование и отладка программного обеспечения» уровня среднего специального образования;

3. разработать и описать элементы содержания обучения и методики преподавания раздела «Организация тестирования программного обеспечения» по дисциплине «Тестирование и отладка программного обеспечения».

Методы исследования: теоретический анализ, моделирование, проектирование, индукция и дедукция, составление библиографии, конспектирование, аннотирование и цитирование, систематизация и обобщение, изучение педагогической документации.

Практическая значимость работы заключается в возможности использовать наработки в дальнейшей преподавательской деятельности педагогами.

Социальная значимость исследования состоит в ознакомлении обучающихся с особенностями организации тестирования программного обеспечения.

Экономическая значимость заключается в подготовке квалифицированных кадров для дальнейшего представления их на рынке труда как высококвалифицированных специалистов, владеющих навыками тестирования программного обеспечения.

Учреждение образования

«Белорусский государственный университет информатики

и радиоэлектроники»

Факультет радиотехники и электроники

УТВЕРЖДАЮ

Заведующий кафедрой ИРТ

*–––––––––––––*Н.И.Листопад

*24.02.2020* –

ЗАДАНИЕ

по курсовому проектированию № КР 1-08 01 01-07 19 ПЗ

Студенту    *Новосёлову Никите Александровичу* *–––––––––––\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

1. Тема *Методическая разработка раздела «Организация тестирования программного обеспечения» по дисциплине «Тестирование и отладка программного обеспечения» уровня среднего специального образования––––––––*

2. Срок сдачи студентом законченного проекта–*26.05.2020* *–––––––––––––––   \_*

3. Исходные данные к проекту *1) Кодекс Республики Беларусь об образовании от 13.01.2011 № 243-З (с изм. и доп.) // Национальный реестр правовых актов Республики Беларусь. – 2011. – № 8/24152; 2) Молчан, Л.В., Славинская, О.В. Методика преподавания общетехнических и специальных дисциплин: электронный ресурс по учебной дисциплине направления специальности 1-08 01 01-07 «Профессиональное обучение (информатика)» / Л.В. Молчан. – [Электронный ресурс] – Минск: БГУИР, 2017; 3) Тестирование и отладка программного обеспечения: типовая учебная программа по учебной дисциплине профессионального компонента типового учебного плана по специальности 2‑40 01 01 «Программное обеспечение информационных технологий»: [утв. постановлением Министерства образования Республики Беларусь от 26.01.2017 №6].–––––––––––––––––––––––––––––––––––––––––––\_–––––––––––––––––––––––––––––––––––––––––– ––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––– ––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––– ––––––––––––––––––––––––––––––––––––––––––––––––*

4. Содержание расчетно-пояснительной записки (перечень вопросов, которые подлежат разработке) *1)–Титульный лист; 2) Реферат; 3) Задание по курсовой работе; 4) Содержание; 5) Введение; 6) Глава 1. Дидактические основы методики преподавания раздела «Организация тестирования программного обеспечения» дисциплины «Тестирование и отладка программного обеспечения» уровня среднего специального образования, 1.1. Организация и проведение обучения на уровне среднего специального образования в учреждениях образования Республики Беларусь, 1.2. Содержание и особенности методики преподавания дисциплины «Организация тестирования программного обеспечения» специальности 2-40 01 01 «Программное обеспечение информационных технологий»; 7) Глава 2. Разработка содержания и элементов методики преподавания дисциплины «Тестирование и отладка программного обеспечения» по разделу «Организация тестирования программного обеспечения», 2.1. Фрагмент учебной программы дисциплины «Тестирование и отладка программного обеспечения» по разделу «Организация тестирования программного обеспечения», 2.2. Фрагмент календарно-тематического плана дисциплины, 2.3. Разработка содержания занятия по разделу программы; 8) Заключение; 9) Список использованных источников; 10) Приложения; 11) Ведомость документов*

5. Перечень графического материала (с точным обозначением обязательных чертежей и графиков) *–нет–––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––– –––*

6. Консультант по проекту (с обозначением разделов проекта)   *доцент кафедры ИРТ, канд. пед. наук, доцент Парафиянович Т.А. –––––– ––––*

7. Дата выдачи задания –*24.02.2020* ––––*––––––––––––––––––––––––––– –––––––*

8. Календарный график работы над проектом на весь период проектирования (с обозначением сроков выполнения и трудоемкости отдельных этапов): *––––– –*

*8.1. Выбор темы, формулирование целей и задач исследования, формирование оглавления, оформление и подписание задания, изучение нормативных правовых актов, учебной, научной литературы по теме – до 09.03.2020 – (5 %)*

*8.2. Проект текста первого параграфа первой главы – до 20.03.2020 – (10 %)*

*8.3. Проект текста второго параграфа первой главы – до 31.03.2020 – (15 %)*

*8.4. Фрагмент учебной программы, проект текста первого параграфа второй главы – до 13.04.2020 – (15 %) .*

*8.5. Фрагмент календарно-тематического плана, проект текста второго параграфа второй главы – до 24.04.2020 – (15 %) . \_\_\_*

*8.6. Разработка и описание занятия, проект текста третьего параграфа второй главы – до 04.05.2020 – (30 %) . \_\_*

*8.7. Оформление и сдача работы на проверку – до 11.05.2020 – (10 %)\_\_\_\_\_\_\_\_*

*8.8. Защита курсовой работы с 20.05.2020 по 26.05.2020\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

РУКОВОДИТЕЛЬ*– –––––––– Т.А. Парафиянович*

Задание принял к исполнению *– 24.02.2020–––––\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(дата и подпись студента)

**Содержание**

|  |  |
| --- | --- |
| Введение | 7 |
| Глава 1. Дидактические основы методики преподавания раздела «Организация тестирования программного обеспечения» дисциплины «Тестирование и отладка программного обеспечения» уровня среднего специального образования | 9 |
| 1.1. Организация и проведение обучения на уровне среднего специального образования в учреждениях образования Республики Беларусь | 9 |
| 1.2. Содержание и особенности методики преподавания дисциплины «Организация тестирования программного обеспечения» специальности 2-40 01 01 «Программное обеспечение информационных технологий» | 18 |
| Глава 2. Разработка содержания и элементов методики преподавания дисциплины «Тестирование и отладка программного обеспечения» по разделу «Организация тестирования программного обеспечения» | 21 |
| 2.1. Фрагмент учебной программы дисциплины «Тестирование и отладка программного обеспечения» по разделу «Организация тестирования программного обеспечения» | 21 |
| 2.2. Фрагмент календарно-тематического плана дисциплины | 22 |
| 2.3. Разработка содержания занятия по разделу программы | 23 |
| Заключение | 27 |
| Список использованных источников | 28 |
| Приложения | 29 |
| Приложение А. Фрагмент перечня действующих типовых учебных планов | 29 |
| Приложение Б. Фрагмент перечня действующих типовых учебных программ | 31 |
| Приложение В. Фрагмент типовой учебной программы дисциплины | 34 |
| Приложение Г. Фрагмент учебной программы дисциплины | 39 |
| Приложение Д. Фрагмент календарно-тематического плана | 49 |
| Приложение Е. План-конспект лекционного занятия «Особенности защиты информации в информационно-справочных системах» | 54 |
| Приложение Ж. План-конспект лекционного занятия «Особенности защиты информации в сложных корпоративных информационных системах» | 66 |
| Приложение И. План-конспект лекционного занятия «Особенности защиты информации в системах электронного документооборота» | 71 |
| Приложение К. План-конспект лабораторного занятия «Защита баз данных средствами СУБД MS Access» | 78 |
| Приложение Л. Инструкция для лабораторного занятия | 82 |
| Приложение М. Презентации лекционных занятий | 88 |
| Ведомость документов | 89 |

**Введение**

Тема данной курсовой работы — «Методическая разработка раздела «Особенности построения системы защиты информации в информационных системах различного типа» по дисциплине «Защита компьютерной информа­ции» уровня среднего специального образования». Данная курсовая работа проектировочного характера, она направлена на то, чтобы обобщить, систе­матизировать и закрепить знания, полученные при изучении предмета «Методика преподавания общетехнических и специальных дисциплин» и применить их на практике при разработке фрагмента курса по учебной дисциплине «Защита компьютерной информации». Курсовая работа способствует формированию умений подбора и анализа литературных источников, использования теоретических знаний при решении практических задач. В подготовке будущего педагога курсовая работа играет огромную роль. Она направлена на формирование системы методических знаний, умений и навыков, дающих возможность целенаправленно, осознанно и эффективно обучать, и воспитывать учащихся.

Для выполнения курсовой работы необходимо система теоретических знаний об этапах обучения и содержании деятельности на каждом из этапов, т.е. умение анализировать учебно-программную документацию: учебный план, учебную программу, квалификационную характеристику. После анализа учебно-программной документации уметь делать правильные выводы для дальнейшего применения их при разработке дидактического материала, написания календарно-тематического плана, плана-конспекта учебного занятия, правильного выбора методов, форм и средств обучения.

Цель работы: обоснование и разработка элементов содержания обучения и методики преподавания раздела «Особенности построения системы защиты информации в информационных системах различного типа» по дисциплине «Защита компьютерной информации» уровня среднего специального образования.

Задачи:

* выявить и описать основные характеристики образовательного процесса уровня среднего специального образования и используемой дидактической системы;
* выявить на основе анализа типовой учебной программы, частных методик, спрогнозировать и описать особенности методики преподавания дисциплины «Защита компьютерной информации» уровня среднего специального образования;
* разработать и описать элементы содержания обучения и методики преподавания раздела «Особенности построения системы защиты информации в информационных системах различного типа» дисциплины «Защита компьютерной информации».

Объектом является образовательный процесс уровня среднего специального образования, предметом является методика преподавания дисциплины «Защита компьютерной информации».

Методы исследования: теоретический анализ педагогической, научно-технической литературы, учебников и учебных пособий, квалификационных характеристик, моделирование; проектирование; обобщение; анализ и обобщение отечественной и зарубежной практики в области профессиональной педагогики.

Представленная работа выполнена самостоятельно на основе источников и литературы, список которых представлен в соответствующем разделе, не содержит плагиата. При выполнении работы использованы источники (в том числе действующие нормативы) 2010-2020 годов.

**Глава 1**

**дидактические основы методики преподавания**

**раздела «особенности построения систем защиты**

**информации в информационных системах**

**различного типа» дисциплины «защита**

**компьютерной информации» уровня**

**среднего специального образования**

* 1. **Организация и проведение обучения на уровне среднего**

**специального образования в учреждениях образования**

**Республики Беларусь**

Согласно Кодексу Республики Беларусь об образовании мы проанали­зировали изучаемый вопрос и сделали выводы, представленные ниже [1].

Среднее специальное образование — уровень основного образования, направленный на развитие личности учащегося, курсанта, получение ими специальной теоретической и практической подготовки, завершающийся присвоением квалификации специалиста со средним специальным образова­нием, рабочего со средним специальным образованием.

Система среднего специального образования включает в себя:

* участников образовательного процесса при реализации образовательных программ среднего специального образования;
* образовательные программы среднего специального образования;
* учреждения среднего специального образования;
* иные учреждения образования, реализующие образовательные программы среднего специального образования;
* государственные организации образования, обеспечивающие функционирование системы среднего специального образования;
* учебно-методические объединения в сфере среднего специального образования;
* организации, обеспечивающие проведение практических занятий, прохождение практики учащимися, курсантами;
* организации — заказчики кадров;
* республиканские органы государственного управления, иные государственные организации, подчиненные Правительству Республики Беларусь, местные исполнительные и распорядительные органы, иные организации и физических лиц в пределах их полномочий в сфере среднего специального образования [1, c.150-151].

Участниками образовательного процесса при реализации образовательных программ среднего специального образования являются учащиеся, курсанты, законные представители несовершеннолетних учащихся, курсантов, педагогические работники.

Учащимся на весь период получения среднего специального образования выдаются билет учащегося и книжка успеваемости учащегося, образцы которых устанавливаются Министерством образования Республики Беларусь.

Курсантам на весь период получения среднего специального образования выдается книжка успеваемости учащегося, образец которой устанавливается Министерством образования Республики Беларусь.

Образовательные программы среднего специального образования подразделяются на:

* образовательную программу среднего специального образования, обеспечивающую получение квалификации специалиста со средним специальным образованием;
* образовательную программу среднего специального образования, обеспечивающую получение квалификации рабочего со средним специальным образованием;
* образовательную программу среднего специального образования, обеспечивающую получение квалификации специалиста со средним специальным образованием и интегрированную с образовательными программами профессионально-технического образования;
* образовательную программу среднего специального образования, обеспечивающую получение квалификации рабочего со средним специальным образованием и интегрированную с образовательными программами профессионально-технического образования [1, c.151].

Образовательная программа среднего специального образования, обеспечивающая получение квалификации специалиста со средним специальным образованием, предусматривает базовый или повышенный уровень изучения учебных дисциплин, прохождения практики.

При освоении содержания образовательных программ среднего специального образования на основе общего базового образования обеспечивается получение общего среднего образования.

При освоении содержания образовательной программы среднего специального образования, обеспечивающей получение квалификации специалиста со средним специальным образованием, в случаях, предусмотренных образовательными стандартами среднего специального образования, осуществляется присвоение квалификации рабочего.

Образовательные программы среднего специального образования реализуются в очной и заочной формах получения образования.

Образовательные программы среднего специального образования реализуются в учреждениях среднего специального образования, профессионально-технических колледжах, гимназиях — колледжах искусств, базовых школах — колледжах искусств, средних школах — колледжах искусств, средних школах — училищах олимпийского резерва, а также могут реализовываться в учреждениях высшего образования. Виды реализуемых образовательных программ среднего специального образования в указанных учреждениях образования [1].

Образовательные стандарты среднего специального образования разрабатываются по каждой специальности (направлению специальности) и устанавливают требования к содержанию профессиональной деятельности специалиста со средним специальным образованием, рабочего со средним специальным образованием, компетентности специалиста со средним специальным образованием, рабочего со средним специальным образованием, содержанию учебно-программной документации образовательных программ среднего специального образования, уровню основного образования лиц, поступающих для получения среднего специального образования, вступительным испытаниям, формам и срокам получения среднего специального образования, организации образовательного процесса, объему учебной нагрузки учащихся, курсантов, уровню подготовки выпускников, итоговой аттестации.

Разработку образовательных стандартов среднего специального образования организует Министерство образования Республики Беларусь и осуществляет ее совместно с учебно-методическими объединениями в сфере среднего специального образования, республиканскими органами государственного управления, иными государственными организациями, подчиненными Правительству Республики Беларусь, в соответствии с перечнем закрепленных за ними специальностей, утверждаемым Правительством Республики Беларусь.

Образовательные стандарты среднего специального образования утверждаются Министерством образования Республики Беларусь по согласованию с республиканскими органами государственного управления, иными государственными организациями, подчиненными Правительству Республики Беларусь, для которых осуществляется подготовка специалистов со средним специальным образованием, рабочих со средним специальным образованием.

Срок получения среднего специального образования в дневной форме получения образования составляет:

1. На основе общего базового образования — от трех до четырех лет;
2. На основе общего среднего образования — от двух до трех лет;
3. На основе профессионально-технического образования с общим средним образованием — от одного года до трех лет [1, c.152-153].

Срок получения среднего специального образования при освоении содержания образовательной программы среднего специального образования, обеспечивающей получение квалификации специалиста со средним специальным образованием и предусматривающей повышенный уровень изучения учебных дисциплин, прохождения практики, срок получе­ния среднего специального образования в вечерней или заочной форме получения образования определяются сроком получения среднего специального образования в дневной форме получения образования и увеличиваются не более чем на один год.

Срок получения среднего специального образования при освоении содержания образовательной программы среднего специального образования, обеспечивающей получение квалификации специалиста со средним специальным образованием, для учащихся средних школ – училищ олимпийского резерва по решению учредителя средней школы – училища олимпийского резерва может быть увеличен по причине участия в течение учебного года в составе национальных и сборных команд Республики Беларусь по видам спорта в спортивных мероприятиях не более чем на два года [1].

Согласно статье 191 Кодекса Республики Беларусь об образовании было выяснено следующее:

«Учреждение среднего специального образования — учреждение образования, которое реализует образовательные программы среднего специального образования, программу воспитания и защиты прав и законных интересов детей, находящихся в социально опасном положении, и может реализовывать образовательные программы профессионально-технического образования, образовательную программу дополнительного образования детей и молодежи, образовательные программы дополнительного образования взрослых, за исключением образовательной программы переподготовки руководящих работников и специалистов, имеющих высшее образование» [1].

Учреждением среднего специального образования является колледж.

Основным структурным подразделением учреждения среднего специального образования, осуществляющим образовательную деятельность, является отделение.

Главой 34 Кодекса Республики Беларусь об образовании была рассмотрена организация образовательного процесса при реализации образовательных программ среднего специального образования [1].

Образовательный процесс при реализации образовательных программ среднего специального образования организуется в учреждениях образования по учебным годам. Учебный год при реализации образовательных программ среднего специального образования делится на семестры, которые завершаются экзаменационными сессиями.

Для учащихся, курсантов устанавливаются:

* каникулы на протяжении учебного года продолжительностью не менее 2 календарных недель;
* летние каникулы продолжительностью не менее 6 календарных недель [1, c.157].

Основной формой организации образовательного процесса при реализации образовательных программ среднего специального образования является учебное занятие: урок, лекция, курсовое проектирование, семинар­ское, лабораторное, практическое и иное занятие. Учебные занятия могут проводиться по сменам. Дополнительно проводятся факультативные занятия, консультации.

Количество часов, отводимых на учебную и производственную практи­ку, составляет не менее 20 процентов от общего количества часов, отводимых на реализацию образовательных программ среднего специального образования.

Порядок организации учебной и производственной практики определяется Положением о практике учащихся, курсантов, осваивающих содержание образовательных программ среднего специального образования, утверждаемым Правительством Республики Беларусь.

Образовательный процесс при реализации образовательных программ среднего специального образования осуществляется в учебных группах или индивидуально.

Наполняемость учебной группы при получении среднего специального образования в дневной форме получения образования составляет от 25 до 30 учащихся, курсантов, в вечерней и заочной формах получения образования – от 15 до 20 учащихся, курсантов.

Наполняемость учебной группы, в которой образовательный процесс организован только для лиц с особенностями психофизического развития, составляет от 6 до 12 учащихся, курсантов.

Наполняемость учебной группы, в которой образовательный процесс одновременно организован для лиц с особенностями психофизического развития и иных лиц, составляет от 15 до 20 учащихся, курсантов, из них не более 6 учащихся, курсантов из числа лиц с особенностями психофизического развития.

Учредитель учреждения образования, реализующего образовательные программы среднего специального образования, может устанавливать меньшую наполняемость групп. При этом для учреждений образования, функционирование которых обеспечивается за счет средств республиканского бюджета, решение об уменьшении наполняемости групп принимается по согласованию с Министерством финансов Республики Беларусь.

В случаях, предусмотренных Положением об учреждении среднего специального образования, учебные группы могут делиться на подгруппы.

Образовательный процесс осуществляется индивидуально на основании решения руководителя учреждения образования, реализующего образовательные программы среднего специального образования, в соответствии с индивидуальным учебным планом или на основании типового учебного плана по специальности (направлению специальности) [1].

Главой 35 Кодекса Республики Беларусь об образовании была рассмотрена аттестация учащихся, курсантов при освоении содержания образовательных программ среднего специального образования [1].

Учащиеся, курсанты при освоении содержания образовательных про­грамм среднего специального образования проходят текущую аттестацию.

Формами текущей аттестации являются:

* опрос учащегося, курсанта;
* контрольная работа;
* курсовой проект (курсовая работа);
* зачет (дифференцированный зачет);
* экзамен по учебной дисциплине [1, c.158].

Результаты текущей аттестации учащихся, курсантов оцениваются отметками в баллах по десятибалльной шкале либо отметками «зачтено», «не зачтено». Положительными являются отметки не ниже 4 (четырех) баллов и «зачтено».

Порядок проведения текущей аттестации учащихся, курсантов при освоении содержания образовательных программ среднего специального образования определяется Правилами проведения аттестации учащихся, курсантов при освоении содержания образовательных программ среднего специального образования.

Учащиеся, курсанты при завершении освоения содержания образовательных программ среднего специального образования проходят итоговую аттестацию.

Итоговая аттестация осуществляется государственной квалификационной комиссией.

Итоговая аттестация проводится в одной из следующих форм:

* защита дипломного проекта;
* государственные экзамены по учебным дисциплинам;
* государственный экзамен по специальности (направлению специальности);
* государственный экзамен по специальности (направлению специальности) и защита дипломного проекта (работы) [1, c.158-159].

К итоговой аттестации допускаются учащиеся, курсанты, выполнившие учебные планы и учебные программы.

Результаты итоговой аттестации учащихся, курсантов оцениваются отметками в баллах по десятибалльной шкале. Положительными являются отметки не ниже 4 (четырех) баллов.

Учащимся, курсантам, не прошедшим итоговую аттестацию в установленный срок по уважительной причине, предоставляется право прохождения итоговой аттестации в другой срок во время работы государственной квалификационной комиссии.

Учащимся, курсантам, не прошедшим итоговую аттестацию в установленный срок без уважительной причины или получившим по ее результатам отметки ниже 4 (четырех) баллов, предоставляется право прохождения итоговой аттестации во время работы государственной квалификационной комиссии, но не ранее чем через десять месяцев.

Порядок проведения итоговой аттестации учащихся, курсантов при освоении содержания образовательных программ среднего специального образования определяется Правилами проведения аттестации учащихся, кур­сантов при освоении содержания образовательных программ среднего специ­ального образования [1].

Была рассмотрена глава 36 Кодекса Республики Беларусь об образовании, где описано научно-методическое обеспечение среднего специального образования [1].

Научно-методическое обеспечение среднего специального образования включает в себя:

* учебно-программную документацию образовательных программ среднего специального образования;
* программно-планирующую документацию воспитания;
* учебно-методическую документацию;
* учебные издания;
* информационно-аналитические материалы [1, с.159].

Научно-методическое обеспечение среднего специального образования осуществляют:

* организации, осуществляющие научно-методическое обеспечение среднего специального образования;
* учреждения среднего специального образования;
* иные учреждения образования, реализующие образовательные программы среднего специального образования;
* учебно-методические объединения в сфере среднего специального образования;
* организации – заказчики кадров;
* республиканские органы государственного управления, иные государственные организации, подчиненные Правительству Республики Беларусь, иные организации и физические лица в пределах их полномочий в сфере среднего специального образования [1, c.159].

Учебно-программная документация образовательных программ среднего специального образования включает в себя учебные планы и учебные программы.

Учебные планы подразделяются на:

* типовые учебные планы по специальностям (направлениям специальностей);
* типовые учебные планы по специализациям;
* учебные планы учреждений образования, реализующих образовательные программы среднего специального образования, по специальностям (направлениям специальностей) и специализациям;
* экспериментальные учебные планы учреждений образования, реализующих образовательные программы среднего специального образования, по специальностям (направлениям специальностей) и специализациям;
* индивидуальные учебные планы [1, с.160].

Типовой учебный план по специальности (направлению специальности) является техническим нормативным правовым актом, разрабатывается на основе образовательного стандарта среднего специально­го образования по специальности (направлению специальности) и устанавливает перечень компонентов, циклов, последовательность изучения учебных дисциплин, количество учебных часов, отводимых на их изучение, формы учебных занятий, виды и сроки прохождения практики, формы и сроки проведения аттестации, минимальное количество обязательных контрольных работ, экзаменов применительно к специальности (направлению специальности), а также перечень необходимых кабинетов, лабораторий, мастерских и иных учебных объектов.

Типовые учебные планы по специальностям (направлениям специальностей) разрабатываются организациями, осуществляющими научно-методическое обеспечение среднего специального образования, и утверждаются Министерством образования Республики Беларусь по согласованию с заинтересованными республиканскими органами государственного управления, иными государственными организациями, подчиненными Правительству Республики Беларусь, в соответствии с перечнем закрепленных за ними специальностей при наличии заключений органов и учреждений, осуществляющих государственный санитарный надзор, об их соответствии санитарно-эпидемиологическому законодательству.

Типовой учебный план по специализации является техническим нормативным правовым актом, разрабатывается как приложение к типовому учебному плану по специальности (направлению специальности), содержит цикл специализации и включает в себя перечень учебных дисциплин специализации, количество учебных часов, отводимых на их изучение, формы учебных занятий, виды и сроки прохождения практики, формы и сроки проведения аттестации по учебным дисциплинам специализации, а также перечень необходимых кабинетов, лабораторий, мастерских и иных учебных объектов.

Типовые учебные планы по специализации разрабатываются организациями, осуществляющими научно-методическое обеспечение среднего специального образования, и утверждаются республиканскими органами государственного управления, иными государственными организациями, подчиненными Правительству Республики Беларусь, в соответствии с перечнем закрепленных за ними специальностей при наличии заключений органов и учреждений, осуществляющих государственный санитарный надзор, об их соответствии санитарно-эпидемиологическому законодательству.

Учебный план учреждения образования, реализующего образовательные программы среднего специального образования, по специальностям (направлениям специальностей) и специализациям разрабатывается учреждением образования, реализующим образовательные программы среднего специального образования, на основе типового учебного плана по специальности (направлению специальности) и типового учебного плана по специализации с учетом уровня изучения учебных дисциплин, прохождения практики и утверждается руководителем этого учреждения об­разования.

Учебный план учреждения образования, реализующего образователь­ные программы среднего специального образования, предусматривающий повышенный уровень изучения учебных дисциплин, прохождения практики, утверждается руководителем этого учреждения образования по согласованию с его учредителем.

Экспериментальный учебный план учреждения образования, реализующего образовательные программы среднего специального образования, по специальности (направлению специальности) и специализации апробируется в учреждении образования, реализующем образовательные программы среднего специального образования, на базе которого осуществляется экспериментальная деятельность.

Экспериментальные учебные планы учреждений образования, реализующих образовательные программы среднего специального образования, по специальностям (направлениям специальностей) и специализациям разрабатываются учреждениями образования, реализующими образовательные программы среднего специального образования, на базе которых осуществляется экспериментальная деятельность, и утверждаются Министерством образования Республики Беларусь по согласованию с учредителями этих учреждений образования.

Индивидуальный учебный план устанавливает особенности получения среднего специального образования одаренными и талантливыми учащимися, курсантами, а также учащимися, курсантами, которые по уважительным причинам не могут постоянно или временно посещать учебные занятия и (или) проходить в установленные сроки аттестацию.

Индивидуальные учебные планы разрабатываются учреждениями образования, реализующими образовательные программы среднего специального образования, на основе учебных планов учреждений образования, реализующих образовательные программы среднего специального образования, по специальностям (направлениям специальностей) и специализациям и утверждаются их руководителями.

Учебные программы подразделяются на:

* типовые учебные программы по учебным дисциплинам;
* типовые учебные программы по практике;
* учебные программы учреждений образования, реализующих образовательные программы среднего специального образования, по учебным дисциплинам;
* учебные программы учреждений образования, реализующих образовательные программы среднего специального образования, по практике;
* экспериментальные учебные программы учреждений образования, реализующих образовательные программы среднего специального образования, по учебным дисциплинам;
* экспериментальные учебные программы учреждений образования, реализующих образовательные программы среднего специального образова­ния, по практике [1, c.161].

Типовая учебная программа по учебной дисциплине является техническим нормативным правовым актом и определяет содержание учебной дисциплины, время, отведенное на изучение отдельных тем, основные требования к результатам учебной деятельности учащихся, курсантов, рекомендуемые формы и методы обучения и воспитания, перечень учебных изданий и средств обучения.

Типовые учебные программы по учебным дисциплинам профессионального компонента разрабатываются организациями, осуществляющими научно-методическое обеспечение среднего специального образования, и утверждаются республиканскими органами государственного управления, иными государственными организациями, подчиненными Правительству Республики Беларусь, в соответствии с перечнем закрепленных за ними специальностей.

Типовые учебные программы по учебным дисциплинам общеобразовательного компонента разрабатываются и утверждаются Министерством образования Республики Беларусь.

Типовая учебная программа по практике является техническим нормативным правовым актом и определяет содержание, сроки и последовательность прохождения учащимися, курсантами практики, основные требования к условиям организации практики, результатам прохождения практики учащимися, курсантами, рекомендуемые формы и методы обучения и воспитания, перечень учебных изданий и средств обучения.

Типовые учебные программы по практике разрабатываются организациями, осуществляющими научно-методическое обеспечение среднего специального образования, и утверждаются республиканскими органами государственного управления, иными государственными организациями, подчиненными Правительству Республики Беларусь, в соответствии с перечнем закрепленных за ними специальностей.

Учебная программа учреждения образования, реализующего образовательные программы среднего специального образования, по учебной дисциплине разрабатывается учреждением образования, реализующим образовательные программы среднего специального образования, на основе типовой учебной программы по учебной дисциплине, предусматривает базовый или повышенный уровень изучения учебной дисциплины и утверждается его руководителем.

Учебная программа учреждения образования, реализующего образовательные программы среднего специального образования, по практике разрабатывается этим учреждением образования на основе типовой учебной программы по практике, предусматривает базовый или повышенный уровень прохождения практики и утверждается его руководителем.

Экспериментальная учебная программа учреждения образования, реа­лизующего образовательные программы среднего специального образования, по учебной дисциплине, экспериментальная учебная программа учреждения образования, реализующего образовательные программы среднего специального образования, по практике апробируются в учреждении образования, реализующем образовательные программы среднего специального образования, на базе которого осуществляется экспериментальная деятельность.

Экспериментальные учебные программы учреждений образования, реализующих образовательные программы среднего специального образования, по учебным дисциплинам, экспериментальные учебные программы учреждений образования, реализующих образовательные программы среднего специального образования, по практике разрабатываются учреждениями образования, реализующими образовательные программы среднего специального образования, на базе которых осуществляется экспериментальная деятельность, и утверждаются Министерством образования Республики Беларусь по согласованию с учредителями этих учреждений образования [1].

* 1. **Содержание и особенности методики преподавания**

**дисциплины «Защита компьютерной информации» специальности**

**2-40 01 01 «Программное обеспечение информационных технологий»**

Содержание и особенности методики преподавания учебной дисциплины «Защита компьютерной информации» специальности 2-40 01 01 «Программное обеспечение информационных технологий» рассмотрены на основе типовой учебной программы, утвержденной постановлением Министерства образования Республики Беларусь от 26.01.2017 №6 [2].

Типовая учебная программа учебной дисциплины «Защита компьютерной информации» (далее — программа) предусматривает изучение методов и алгоритмов защиты компьютерной информации в информационных системах различного назначения.

Цель преподавания учебной дисциплины — развитие профессиональной компетентности в области разработки, анализа и эксплуатации средств защиты компьютерной информации.

Изучение программного учебного материала базируется на знаниях, полученных учащимися в ходе изучения таких учебных дисциплин, как «Математика», «Теория вероятностей и математическая статистика», «Системное программное обеспечение».

Для закрепления теоретического материала и формирования у учащихся необходимых умений и навыков программой предусматривается проведение лабораторных занятий. Форма проведения лабораторных занятий определяется преподавателем исходя из цели обучения и содержания учебного материала.

В целях контроля усвоения учебного материала предусматривается проведение одной обязательной контрольной работы (ОКР). Содержание и конкретные сроки проведения ОКР определяются преподавателем, обсуждаются на заседании предметной (цикловой) комиссии и утверждаются в установленном порядке.

Программой определены цели изучения каждой темы, спрогнозирова­ны результаты их достижения в соответствии с уровнями усвоения учебного материала.

В результате изучения учебной дисциплины учащиеся должны:

1. Знать на уровне представления:

* особенности функционирования межсетевых экранов;
* способы защиты информации;
* технологии анализа защищенности и обнаружения атак;

1. Знать на уровне понимания:
   * алгоритмы блочного шифрования;
   * алгоритмы асимметричного шифрования;
   * алгоритмы электронной цифровой подписи;
   * алгоритмы идентификации и проверки подлинности;
2. Уметь:
   * шифровать данные классическими криптосистемами;
   * защитить персональный компьютер от несанкционированного доступа;
   * скрывать информацию на персональном компьютере;
   * использовать программное обеспечение для шифрова­ния/дешифрования файлов, частей или всего винчестера;
   * создавать виртуальные зашифрованные диски [2, c.27].

В программе приведены примерные критерии оценки результатов учебной деятельности учащихся по учебной дисциплине, которые разработаны на основе десятибалльной шкалы и показателей оценки результатов учебной деятельности обучающихся в учреждениях среднего специального образования.

Программа содержит примерный перечень оснащения лаборатории техническими и программными средствами, необходимыми для обеспечения образовательного процесса.

Приведенный в программе тематический план является рекомендательным. Предметная (цикловая) комиссия учреждения образования может вносить обоснованные изменения в содержание и последовательность изложения программного учебного материала, распределение учебных часов по темам в пределах общего бюджета времени, отведенного на изучение учебной дисциплины. Все изменения должны быть утверждены заместителем руководителя учреждения образования по учебной работе.

**Глава 2**

**Разработка содержания и элементов методики**

**преподавания дисциплины «Защита компьютерной информации» по разделу «особенности построения систем защиты информации в информационных**

**системах различного типа»**

**2.1. Фрагмент учебной программы дисциплины «Защита компьютерной информации» по разделу «Особенности построения систем защиты**

**информации в информационных системах различного типа»**

Данный фрагмент учебной программы был разработан на основе типовой учебной программы по дисциплине «Защита компьютерной информации» утвержденной Министерством Образования Республики Беларусь 26 января 2017 году. Типовая учебная программа по дисциплине «Защита компьютерной информации» представлена в перечне действующих типовых учебных программ специальности 2-40 01 01 «Программное обеспечение информационных технологий» [3]. Перечень программ специальности 2‑40 01 01 «Программное обеспечение информационных технологий» подтвержден типовым учебным планом данной специальности [4]. Фрагмент перечня действующих типовых учебных планов представлен в приложении А, и фрагмент перечня действующих типовых учебных программ представлен в приложении Б.

Типовая учебная программа по учебной дисциплине является техническим нормативным правовым актом и определяет содержание учебной дисциплины, время, отведенное на изучение отдельных тем, основные требования к результатам учебной деятельности учащихся, курсантов, рекомендуемые формы и методы обучения и воспитания, перечень учебных изданий и средств обучения.

Типовые учебные программы по учебным дисциплинам профессионального компонента разрабатываются организациями, осуществляющими научно-методическое обеспечение среднего специального образования, и утверждаются республиканскими органами государственного управления, иными государственными организациями, подчиненными Правительству Республики Беларусь, в соответствии с перечнем закрепленных за ними специальностей.

Учебная программа учреждения образования, реализующего образовательные программы среднего специального образования, по учебной дисциплине разрабатывается учреждением образования, реализующим образовательные программы среднего специального образования, на основе типовой учебной программы по учебной дисциплине, предусматривает базовый или повышенный уровень изучения учебной дисциплины и утверждается его руководителем.

Разработанный фрагмент учебной программы состоит из:

* примерно-тематического плана;
* пояснительной записки;
* содержания дисциплины;
* литературы.

В примерно-тематическом плане указывается распределение часов на изучение дисциплины по разделам и темам.

Утвержденная учебная программа дисциплины «Защита компьютерной информации» представлена в приложении В.

Разработанный фрагмент учебной программы дисциплины «Защита компьютерной информации» представлен в приложении Г.

Основная часть содержание программы представляет собой таблицу из трех основных столбцов, в которых указываются цели изучения тем, их со­держание и результат изучения. При составлении календарно-тематического плана и дальнейшего проведения занятий преподаватель должен руковод­ствоваться содержанием программы. То есть разработанные преподавателем учебные занятия, выбранные их организационные формы и методы обучения должны быть оптимальны, и направлены на достижения целей и результатов учебной программы.

**2.2. Фрагмент календарно-тематического плана дисциплины**

На титульном листе календарно-тематического плана предусмотреть гриф «УТВЕРЖДАЮ», прописать наименование учебной дисциплины, номер групп, указать форму обучения, фамилию, имя и отчество преподавателя, дату утверждения учебной программы, в соответствии с которой составлен календарно-тематический план, количество учебных часов по учебному плану, отведенных на изучение учебной дисциплины, в том числе на проведение обзорных, лабораторных, практических занятий, на курсовое проектирование.

Указать количество домашних контрольных работы по учебной дисциплине.

На первой странице в графе 1 записывается порядковый номер учебного занятия.

Графы 2, 3, 4, 5, 6 заполняются в соответствии с расписанием учебных занятий для каждой учебной группы.

В графу 7 «Наименование разделов, тем по учебной программе, тем отдельных учебных занятий» вписываются названия разделов, тем, отдельных учебных занятий программного материала, наиболее сложного, трудно усваиваемого, требующего конкретизации, объяснения и обобщения со стороны преподавателя, рассматриваемый на обзорных, лабораторных и практических занятиях. Содержательная и исполнительная часть лабораторных и практических занятий (работ) должна быть наполнена деятельностью учащихся, направленной на закрепление теоретических знаний на практике, на формирование профессиональных умений и навыков пользования установками, оборудованием, приборами и т.д.

В графе 8 указывается количество учебных часов, предусмотренных на проведение учебного занятия. Учебный материал по учебной дисциплине разбивается на темы (подтемы), рассчитанные, как правило, на 2 учебных часа.

На второй странице в графе 9 указывается тип учебного занятия.

В графе 10 указывается учебно-методическое обеспечение учебного занятия (средства обучения) в соответствии с выбранным методом учебно-познавательной деятельности.

В графу 11 пописываются задания для самостоятельной работы учащихся (наименование тем учебной программы учебной дисциплины, выдаваемые учащимся для самостоятельного изучения, графические расчеты и другие задания, а также задания для проведения практических и лабораторных работы), как в межсессионный период, так и в период лабораторно-экзаменационных сессий.

В графу 12 вносится основная и дополнительная литература, методические пособия, практикумы, конспекты лекций и электронный адрес, по которому учащиеся могут получить дополнительную информацию по изучению учебной дисциплины.

В графу 13 прописываются коррективы, внесенные с учетом достижений науки и техники, изменений, вносимых с содержание типовой учебной программы учебной дисциплины и др. Изменения в дополнения должны быть обсуждены на заседании предметной (цикловой) комиссии, утверждены заместителем директора по учебной работе.

На последней странице размещается раздел «Литература», который, как правило, представляется следующими подразделами: «Основная литература», «Дополнительная литература». В подразделы вносятся учебники и другие печатные текстовые средства, специальное учебно-методическое обеспечение, практикумы по лабораторным и практическим занятиям (работам), автоматизированные обучающие курсы, профессиональные прикладные программы электронные источники учебной информации и др.

Календарно-тематический план составляется на учебный год (семестр), рассматривается предметной (цикловой) комиссией и утверждается заместителем директора по учебной работе.

Разработанный фрагмент календарно-тематического плана представлен в приложении Д.

**2.3. Разработка содержания занятия по разделу программы**

В процессе разработки содержания занятия по разделу программы был изучен образовательный стандарт среднего специального образования по специальности 2-40 01 01 «Программное обеспечение информационных технологий», а также была рассмотрена разработка учебных программ допрофессиональной и профессиональной подготовки учащихся учреждений общего среднего и специального образования [5].

Согласно курсовому проекту необходимо разработать три лекционных занятия, а также одно лабораторное занятие в условиях лекционно-семинарской дидактической системы. В данной работе предложено содержа­ние лабораторной работы № 1 учебной программы «Защита баз данных сред­ствами СУБД MS Access».

На данный момент традиционная педагогика предлагает несколько способов организации занятий по отработке навыков и два из них – лекционные и лабораторные занятия. На лекционных занятиях учащиеся приобретают новые знания, на лабораторных – развивают свою учебную и познавательную деятельность в специально созданных для этого условиях. Сначала рассмотрим лекционные занятия.

По характеру лекционное занятие относится к лекционно-семинарским формам обучения.

В начале занятия педагог сообщает тему и цели занятия, мотивирует учащихся на успешную учебную деятельность.

В конце занятия педагог обсуждает с учащимися результаты их теоретической деятельности, спрашивает, что было непонятно, что вызвало трудности, при необходимости отвечает на вопросы, возникшие у учащихся.

Учащиеся должны иметь при себе конспект для записи лекции, предварительно повторить предыдущий материал для качественного усвоения материала.

Процесс приобретения знаний в рамках образовательного процесса осуществляется по следующей схеме:

1. Лекционное занятие, которое включает: ознакомление с новым материалом и конспектирование лекции учащимися.
2. Обсуждение результатов проведенного лекционного занятия (преподавателем и учащимися).
3. Оценка теоретической познавательной деятельности.

Таким образом, лекционное занятие является важной составляющей процесса обучения. В ходе его проведения у учащихся формируются умения и навыки анализировать и делать выводы из наблюдений. Проявляются такие качества личности как терпение, культура поведения и находчивость.

Разработанный план-конспект лекционного занятия «Особенности защиты информации в информационно-справочных системах» представлен в приложении Е, план-конспект лекционного занятия «Особенности защиты информации в сложных корпоративных информационных системах» — в приложении Ж, план-конспект лекционного занятия «Особенности защиты информации в системах электронного документооборота» — в приложении И. Каждый из разработанных план-конспектов содержит название дисциплины, тему учебного занятия, форму проведения учебного занятия, поставленные при разработке цели лекции: обучающая, воспитательная и развивающая. Также стоит отметить, что для структурирования и повышения качества изложения лекционного материала, содержание материала систематизировано в соответствии с разработанным планом каждой лекции.

Теперь рассмотрим лабораторные занятия.

Лабораторные работы планируются в процессе изучения наиболее сложных тем учебной дисциплины, если необходимо разъяснение или подтверждение сущности законов, процессов, явлений, проведение эксперимента и т. д.

Лабораторная работа может выполняться после прохождения всего теоретического курса (последовательный метод) или в процессе его освоения (параллельный метод). Организационно такие занятия могут быть фронтальными (когда все обучающиеся выполняют одну и ту же работу) или групповыми (когда обучающиеся разделены на небольшие подгруппы из 2–5 человек, выполняющие разные работы) [6, с.4].

Лабораторные работы по учебным дисциплинам теоретического обучения носят как иллюстративный, так и исследовательский характер [6, с.5].

Иллюстративный характер проявляется в том, что обучающиеся в процессе проведения опытов воспроизводят то, что им известно из теоретических учебных занятий или учебных пособий. Исследовательский характер заключается в том, что на основании опытов практической деятельности обучающиеся делают самостоятельные выводы [6, с.5].

По характеру занятия лабораторная работа также относится к лекционно-семинарским формам обучения. Она также содержит элемент самостоятельной работы учащихся.

Учащиеся должны быть заранее предупреждены о предстоящей лабораторной работе. Их задача состоит в подготовке к данному виду работы. Они должны просмотреть материал в учебных пособиях, своих конспектах, дополнительной литературе, при необходимости проконсультироваться с преподавателем. Далее практические действия учащийся совершает на занятии самостоятельно под контролем преподавателя. Учащиеся успешно справятся с работой, если будут знать порядок её выполнения. Им надо не только рассказать, но и показать, как лучше выполнить работу.

В начале занятия преподаватель сообщает тему и цели занятия, мотивирует учащихся на успешную учебную деятельность.

В конце занятия преподаватель обсуждает с учащимися результаты их практической деятельности, спрашивает, что было непонятно, что вызвало трудности, при необходимости отвечает на вопросы, возникшие у учащихся. Далее преподаватель принимает отчеты о выполненной работе, выставляет учащимся отметки и сообщает о результатах достижения целей занятия.

Процесс приобретения навыков в рамках образовательного процесса осуществляется по следующей схеме:

1. Практическое занятие, которое включает ознакомление с предстоя­щей работой и практическую деятельность учащихся.
2. Обсуждение результатов практической деятельности (преподавателем и учащимися)
3. Оценка результатов практической деятельности.

Несомненно, многолетняя практика такой схемы преподавания прикладных дисциплин оправдывает себя.

Таким образом, лабораторная работа является важной составляющей процесса обучения. В ходе выполнения у учащихся формируются умения и навыки работы с прикладными программами, вырабатываются самостоятельность, а также способность анализировать и делать выводы из наблюдений. Проявляются такие качества личности как терпение, усидчивость, целеустремлённость и может быть даже находчивость, а также самостоятельность и ответственность.

Разработанный план-конспект лабораторного занятия «Защита баз данных средствами СУБД MS Access» представлен в приложении К.

Разработанная инструкция к лабораторному занятию представлена в приложении Л.

Разработанные презентации к лекционным занятиям «Особенности защиты информации в информационно-справочных системах», «Особенности защиты информации в сложных корпоративных информационных системах» и «Особенности защиты информации в системах электронного документооборота» представлены в приложении М.

**Заключение**

В ходе курсовой работы были рассмотрены дидактические основы ме­тодики преподавания раздела «Особенности построения систем защиты информации в информационных системах различного типа» дисциплины «Защита компьютерной информации» уровня среднего специального образования, а также разработано содержание и элементы методик преподавания дисциплины «Защита компьютерной информации» по разделу «Особенности построения систем защиты информации в информационных системах различного типа».

Цели и задачи исследования выполнены.

В данной курсовой работе были:

а) выявлены и описаны основные характеристики образовательного процесса уровня среднего специального образования;

б) на основе анализа типовой учебной программы, частных методик, были выявлены, спрогнозированы и описаны особенности методики преподавания раздела «Особенности построения систем защиты информации в информационных системах различного типа» дисциплины «Защита компьютерной информации» уровня среднего специального образования;

в) разработаны:

1. фрагмент учебной программы,
2. фрагмент календарно-тематического плана и содержания
3. лекционное занятие по теме «Особенности защиты информации в информационно-справочных системах»,
4. лекционное занятие по теме «Особенности защиты информации в сложных корпоративных информационных системах»,
5. лекционное занятие по теме «Особенности защиты информации в системах электронного документооборота», а также
6. лабораторное занятие по теме «Защита баз данных средствами СУБД MS Access».

Все разработанные в курсовой работе учебно-программные документы, их фрагменты находятся во взаимосвязи, соответствуют друг другу.

При разработке элементов обучения были проанализированы и использованы современная учебно-программная документация, учебно-методические источники и нормативно-правовые акты, Кодекс Республики Беларусь об образовании.

Данные элементы обучения могут быть использованы при проведении занятий по дисциплине «Защита компьютерной информации» в учреждениях со средним специальным образованием, обеспечивающих обучение по специальности 2-40 01 01 «Программное обеспечение информационных технологий».

**Список использованных источников**

[1] Кодекс Республики Беларусь об образовании от 13.01.2011 № 243-З (с изм. и доп.) // Национальный реестр правовых актов Республики Беларусь. – 2011. – № 2/1795.

[2] Защита компьютерной информации: типовая учебная программа по учебной дисциплине профессионального компонента типового учебного пла­на по специальности 2-40 01 01 «Программное обеспечение информационных технологий»: утверждено постановлением Министерства образования Республики Беларусь от 26.01.2017 №6 // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. - Режим доступа: http://pravo.by/upload/docs/op/W21731760p\_1489179600.pdf - Дата доступа: 28.04.2020.

[3] Перечень действующих типовых учебных программ по учебным дисциплинам профессионального компонента и практике, типовых учебных планов по специальностям (направлениям специальностей), закрепленных за Министерством образования Республики Беларусь, для учреждений образования, реализующих образовательные программы среднего специального образования: утверждено постановлением Министерства образования Республики Беларусь от 21.08.2019 // Образовательный портал «Профессиональное образование» [Электронный ресурс]. - Режим доступа: http://ripo.unibel.by/index.php?id=1657 - Дата доступа: 28.04.2020.

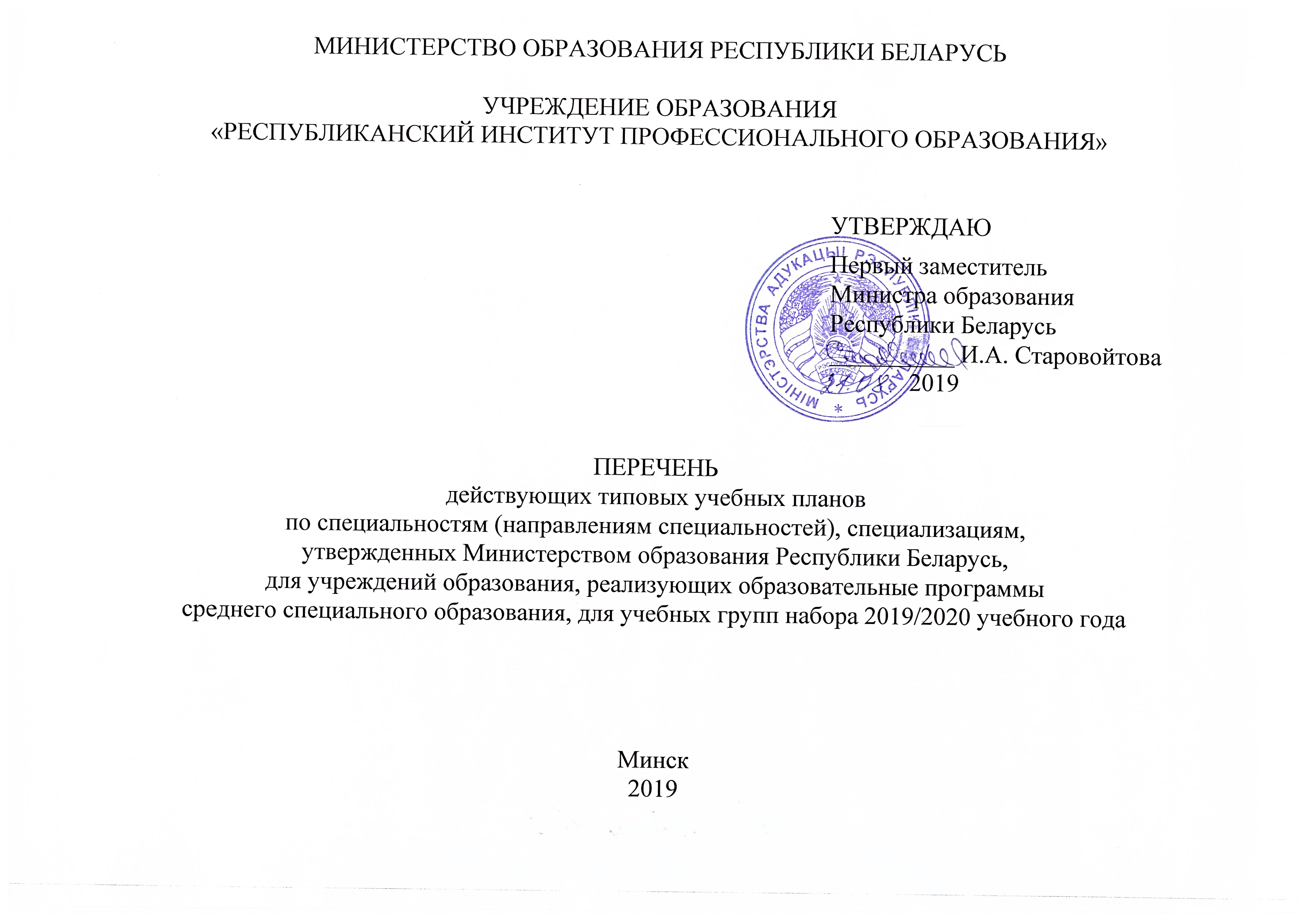
[4] Перечень действующих типовых учебных планов по специальностям (направлениям специальностей), специализациям, утвержденных Министерством образования Республики Беларусь, для учреждений образования, реализующих образовательные программы среднего специального образования, для учебных групп набора 2019/2020 учебного года: утверждено постановлением Министерства образования Республики Беларусь от 21.08.2019 // Образовательный портал «Профессиональное образование» [Электронный ресурс]. - Режим доступа: http://ripo.unibel.by/index.php?id=1656 - Дата доступа: 28.04.2020.

[5] Образовательный стандарт среднего специального образования по специальности 2-40 01 01 «Программное обеспечение информационных технологий»: ОС РБ 2-40 01 01-2014. – Утв. постановлением Министерства образования Респ. Беларусь № 54 от 28.04.2014 г. – Минск : М-во обр. Респ. Беларусь : УО РИПО, 2014. – 30с.

[6] Ильин, М.В. Разработка учебных программ допрофессиональной и профессиональной подготовки учащихся учреждений общего среднего и специального образования : метод. рекомендации / М. В. Ильин, А. Н. Петрова, П. Н. Сидорович ; под общ. ред. М. В. Ильина. – Минск : РИПО, 2019. – 44 c.

Приложение А

**Фрагмент перечня действующих типовых учебных планов**



**ПЕРЕЧЕНЬ**

**действующих типовых учебных планов по специальностям (направлениям специальностей), специализациям,   
утвержденных Министерством образования Республики Беларусь, для учреждений образования,   
реализующих образовательные программы среднего специального образования,  
для учебных групп набора 2019/2020 учебного года**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код профиля и направления образования, группы специальностей, специальности, направления специальности, спе­циализации | Наименование специальности,  направления специальности,  специализации | Типовые учебные планы по специальностям (направлениям специальностей) и специализациям | | Примечание |
| Регистрационный  индекс | Дата утверждения и номер постановления |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **40** | **ИНФОРМАТИКА И вычисли­тельная техника** |  |  |  |
| ***40 01*** | ***программные средства и математические*** |  |  |  |
| 2-40 01 01 | Программное обеспечение информационных технологий | РБ ст. № 930 Д/тип. | 14.05.2019 № 50 |  |
| 2-40 01 01 31 | Программирование для систем автоматизированного проектирования | РБ ст. № 931/930 Д/тип.спец.31 |  |



Начальник Главного управления

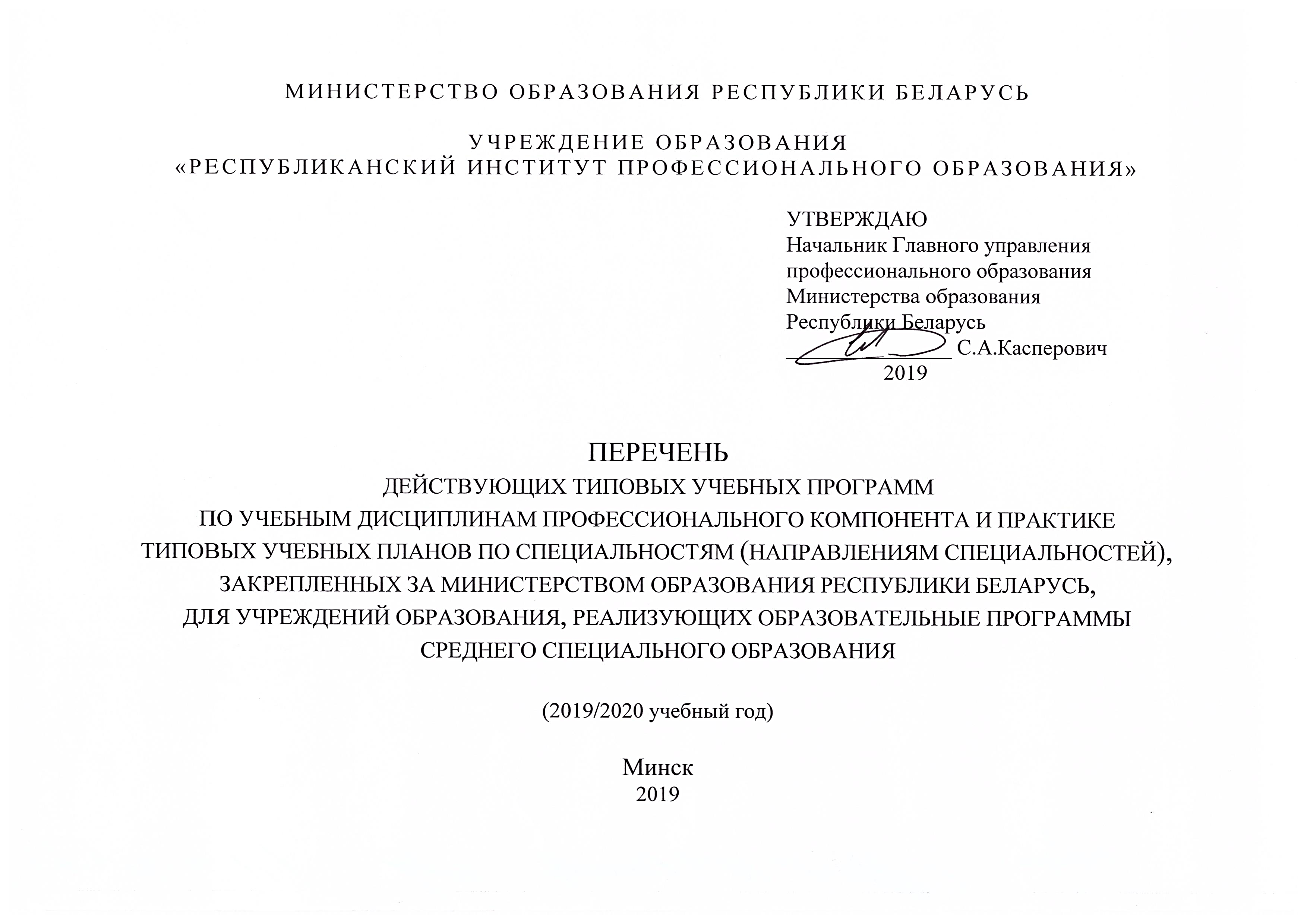
профессионального образования

Министерства образования Республики Беларусь С.А.Касперович

Ректор учреждения образования

Приложение Б

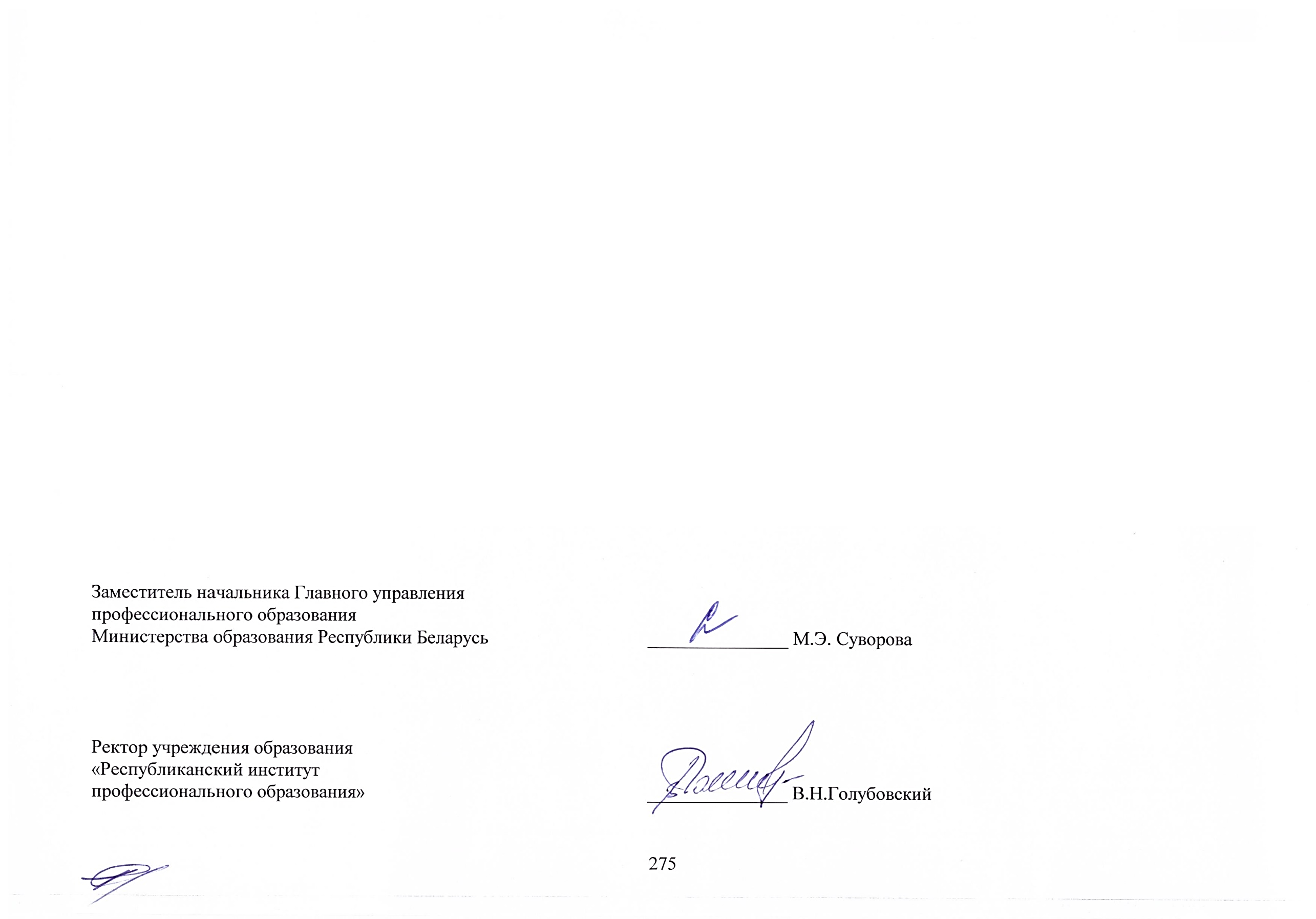
**Фрагмент перечня действующих типовых учебных программ**



**Специальность 2-40 01 01 «Программное обеспечение информационных технологий»**

**Типовой учебный план РБ ст. № 930 Д/тип., утвержденный постановлением Министерства образования Республики Беларусь 14.05.2019 №50**

| Наименование типовых учебных программ | Количество учебных часов по | | Год  утверждения | Кем утверждена | Примечание |
| --- | --- | --- | --- | --- | --- |
| типовому  учебному  плану | типовой  учебной  программе |
| 1. Основы инженерной графики | 40 | 40 | 2019 | Министерством образования  Республики Беларусь |  |
| 1. Математика | 190 | 230 | 2014 | Министерством образования  Республики Беларусь |  |
| 1. Основы алгоритмизации и программирование | 190 |  |  |  | ПТП |
| 1. Теория вероятностей и математическая ста­тистика | 62 |  |  |  | ПТП |
| 1. Арифметико-логические основы вычисли­тельной техники | 106 |  |  |  | ПТП |
| 1. Инструментальное программное обеспечение | 112 |  |  |  | ПТП |
| 1. Стандартизация и сертификация программного обеспечения | 40 |  |  |  | ПТП |
| 1. Охрана труда | 60 | 60 | 2012 | Министерством образования  Республики Беларусь |  |
| 1. Охрана окружающей среды и энергосбережение | 40 | 40 | 2019 | Министерством образования  Республики Беларусь |  |
| 1. Основы предпринимательской деятельности и управления проектами | 96 |  |  |  | ПТП |
| 1. Техника коммуникации и основы командообразования | 72 |  |  |  | ПТП |
| 1. Белорусский язык (профессиональная лексика) | 20 | 20 | 2016 | Министерством образования Республики Беларусь |  |
| 1. Иностранный язык (профессиональная лексика) | 130 |  |  |  | ПТП |
| 1. Конструирование программ и языки программирования | 176 | 176 | 2017 | Министерством образования  Республики Беларусь |  |
| 1. Базы данных и системы управления базами данных | 176 |  |  |  | ПТП |
| 1. Технология разработки программного обеспечения | 144 |  |  |  | ПТП |
| 1. Тестирование программного обеспечения | 100 |  |  |  | ПТП |
| 1. Защита компьютерной информации | 96 | 96 | 2017 | Министерством образования  Республики Беларусь |  |
| 1. Компьютерные сети | 114 | 114 | 2019 | Министерством образования  Республики Беларусь |  |
| 1. Программные средства создания Интернет-приложений | 114 |  |  |  | ПТП |
| 1. Учебная и производственная практика |  |  |  |  | ПТП |



Заместитель начальника Главного управления

профессионального образования

Министерства образования Республики Беларусь \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.Э. Суворова

Ректор учреждения образования

«Республиканский институт

профессионального образования» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение В

**Фрагмент типовой учебной программы дисциплины**

МИНИИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

**УТВЕРЖДЕНО**

Постановление

Министерства образования

Республики Беларусь

26.01.2017 №6

**ТИПОВАЯ УЧЕБНАЯ ПРОГРАММА**

**ПО УЧЕБНОЙ ДИСЦИПЛИНЕ (фрагмент)**

**«**ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

профессионального компонента типового учебного плана

по специальности 2-40 01 01

«Программное обеспечение информационных технологий»

для реализации образовательной программы среднего специального

образования, обеспечивающей получение квалификации специалиста

со средним специальным образованием

Минск

2017

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Типовая учебная программа учебной дисциплины «Защита компьютерной ин­формации» (далее — программа) предусматривает изучение методов и алгоритмов защиты компьютерной информации в информационных системах различного назначения.

Изучение программного учебного материала базируется на знаниях, получен­ных учащимися в ходе изучения таких учебных дисциплин, как «Математика», «Теория вероятностей и математическая статистика», «Системное программное обеспечение».

В процессе преподавания учебной дисциплины необходимо знакомить учащихся с основными понятиями защиты компьютерной информации, со способами и принципами ее осуществления.

Цели изучения учебной дисциплины

образовательные:

– обеспечить получение знаний по защите компьютерной информации и формирование умений и навыков защиты информации с использованием современных технологий и подходов;

– способствовать развитию логического мышления;

– сформировать умения использовать программное обеспечение для шифрования/дешифрования файлов, частей или всего винчестера;

– отработать навыки работы с алгоритмами шифрования;

развивающие:

– обеспечить условия для развития внимательности, наблюдательности и умений выделять главное в защите компьютерной информации, оценке различных процессов, явлений и фактов;

– способствовать развитию умений учащихся обобщать полученные знания, проводить анализ, синтез, сравнения, делать необходимые выводы;

– способствовать развитию умений творческого подхода к решению практических задач;

– развивать критическое мышление, групповую самоорганизацию, умение вести диалог;

воспитательные:

– создать условия, обеспечивающие воспитание интереса к будущей профессии;

– обеспечить условия для воспитания творческого отношения к избранной профессии;

– воспитание трудолюбия, инициативности и настойчивости в преодолении трудностей;

– сформировать умения общаться и работать в команде.

Для закрепления теоретического материала и формирования у учащихся необходимых умений и навыков программой предусматривается проведение лабораторных занятий. Форма проведения лабораторных занятий определяется преподавателем исходя из цели обучения и содержания учебного материала.

В целях контроля усвоения учебного материала предусматривается проведение одной обязательной контрольной работы (ОКР). Содержание и конкретные сроки проведения ОКР определяются преподавателем, обсуждаются на заседании предметной (цикловой) комиссии и утверждаются в установленном порядке.

Программой определены цели изучения каждой темы, спрогнозированы результаты их достижения в соответствии с уровнями усвоения учебного материала.

В результате изучения учебной дисциплины учащиеся в области защиты компьютерной информации должны:

знать на уровне представления:

– особенности функционирования межсетевых экранов;

– способы защиты информации;

– технологии анализа защищенности и обнаружения атак;

знать на уровне понимания:

– алгоритмы блочного шифрования;

– алгоритмы асимметричного шифрования;

– алгоритмы электронной цифровой подписи;

– алгоритмы идентификации и проверки подлинности;

уметь:

– шифровать данные классическими криптосистемами;

– защитить персональный компьютер от несанкционированного доступа;

– скрывать информацию на персональном компьютере;

– использовать программное обеспечение для шифрования/дешифрования файлов, частей или всего винчестера;

– создавать виртуальные зашифрованные диски.

Дисциплина «Защита компьютерной информации» рассчитана на 21 часов занятий (17 часов лекций и 4 часа лабораторных занятий).

**ПРИМЕРНЫЙ** ТЕМАТИЧЕСКИЙ ПЛАН

|  |  |  |
| --- | --- | --- |
| Раздел, тема | Количество часов | |
| всего | в том числе  на ла­бора­торные  работы |
| **Введение** | **1** |  |
| Раздел 1. **Защита информации в информационно-вычислительных системах** | **5** |  |
| 1.1. Проблемы защиты компьютерной информации | 1 |  |
| 1.2. Угрозы безопасности информации в информационно-вычислительных системах | 2 |  |
| 1.3. Основные направления использования средств и методов защиты информации | 2 |  |
| Раздел 2. **Правовые и организационные методы защиты информации в информационно-вычислительных системах** | **4** |  |
| 2.1. Правовое регулирование в области безопасности информации. Характеристика организационных методов защиты | 2 |  |
| 2.2. Стандарты и спецификации в области информационной безопасности | 2 |  |
| Раздел 3. **Методы идентификации и аутентификации** | **8** | **4** |
| 3.1. Идентификация и аутентификация | 2 |  |
| 3.2. Парольные системы идентификации и аутентификации пользователей | 6 |  |
| Раздел 4. **Криптографическая защита компьютерной информации** | **40** | **22** |
| 4.1. Принципы криптографической защиты информации | 2 |  |
| 4.2. Симметричные криптосистемы | 23 | 14 |
| 4.3. Асимметричные криптосистемы | 6 | 4 |
| 4.4. Криптографические функции хеширования | 6 | 4 |
| 4.5. Алгоритмы электронной цифровой подписи | 2 |  |
| *Обязательная контрольная работа* | 1 |  |
| Раздел 5. **Системы защиты программных средств** | **18** | **10** |
| 5.1. Виды вредоносных программных средств | 2 |  |
| 5.2. Защита от компьютерных вирусов | 4 | 2 |
| 5.3. Системы защиты ПО | 12 | 8 |
| Раздел 6. **Политика безопасности** | **4** |  |

|  |  |  |
| --- | --- | --- |
| Раздел, тема | Количество часов | |
| всего | в том числе  на ла­бора­торные  работы |
| 6.1. Структура политики безопасности организации | 2 |  |
| 6.2. Модели основных типов политики безопасности | 2 |  |
| Раздел 7. **Особенности построения систем защиты информации в информационных системах различного типа** | **16** | **4** |
| 1.1. Особенности защиты информации в информационно-справочных системах | 6 |  |
| Лабораторная работа №1  Защита баз данных средствами СУБД MS Access |  | 4 |
| 1.2. Особенности защиты информации в сложных корпоративных информационных системах | 2 |  |
| 1.3. Безопасность работы в сети Интернет | 6 |  |
| 1.4. Особенности защиты информации в системах электронного документооборота | 2 |  |
| **Итого** | **96** | **40** |

Приложение Г

**Фрагмент учебной программы дисциплины**

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

ФИЛИАЛ БЕЛОРУССКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

«МИНСКИЙ РАДИОТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

**УТВЕРЖДАЮ**

Директор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ф.И.О

«\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

      (дата утверждения)

Регистрационный № \_\_\_\_\_\_\_\_\_

ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Учебная программа

для учреждений, обеспечивающих получение среднего специального

образования по специальности

2-40 01 01 «Программное обеспечение информационных технологий»

Минск, 2020

СОСТАВИТЕЛЬ:\_\_\_Сабило В.А.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Предметно-методической комиссией «\_\_\_\_\_\_\_\_\_» Учреждения образования «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_» (протокол № \_\_\_ от \_\_\_. \_\_\_\_\_\_202\_\_ г.)

Педагогическим советом Учреждения образования «\_\_\_\_\_\_\_\_\_\_\_» (протокол №\_\_\_от\_\_\_.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.202\_\_\_ г.)

Методическая экспертиза \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (ФИО методист УМО)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Типовая учебная программа учебной дисциплины «Защита компьютерной ин­формации» (далее — программа) предусматривает изучение методов и алгоритмов защиты компьютерной информации в информационных системах различного назначения.

Изучение программного учебного материала базируется на знаниях, получен­ных учащимися в ходе изучения таких учебных дисциплин, как «Математика», «Теория вероятностей и математическая статистика», «Системное программное обеспечение».

В процессе преподавания учебной дисциплины необходимо знакомить учащихся с основными понятиями защиты компьютерной информации, со способами и принципами ее осуществления.

Цели изучения учебной дисциплины

образовательные:

– обеспечить получение знаний по защите компьютерной информации и формирование умений и навыков защиты информации с использованием современных технологий и подходов;

– способствовать развитию логического мышления;

– сформировать умения использовать программное обеспечение для шифрования/дешифрования файлов, частей или всего винчестера;

– отработать навыки работы с алгоритмами шифрования;

развивающие:

– обеспечить условия для развития внимательности, наблюдательности и умений выделять главное в защите компьютерной информации, оценке различных процессов, явлений и фактов;

– способствовать развитию умений учащихся обобщать полученные знания, проводить анализ, синтез, сравнения, делать необходимые выводы;

– способствовать развитию умений творческого подхода к решению практических задач;

– развивать критическое мышление, групповую самоорганизацию, умение вести диалог;

воспитательные:

– создать условия, обеспечивающие воспитание интереса к будущей профессии;

– обеспечить условия для воспитания творческого отношения к избранной профессии;

– воспитание трудолюбия, инициативности и настойчивости в преодолении трудностей;

– сформировать умения общаться и работать в команде.

Для закрепления теоретического материала и формирования у учащихся необходимых умений и навыков программой предусматривается проведение лабораторных занятий. Форма проведения лабораторных занятий определяется преподавателем исходя из цели обучения и содержания учебного материала.

В целях контроля усвоения учебного материала предусматривается проведение одной обязательной контрольной работы (ОКР). Содержание и конкретные сроки проведения ОКР определяются преподавателем, обсуждаются на заседании предметной (цикловой) комиссии и утверждаются в установленном порядке.

Программой определены цели изучения каждой темы, спрогнозированы результаты их достижения в соответствии с уровнями усвоения учебного материала.

В результате изучения учебной дисциплины учащиеся в области защиты компьютерной информации должны:

знать на уровне представления:

– особенности функционирования межсетевых экранов;

– способы защиты информации;

– технологии анализа защищенности и обнаружения атак;

знать на уровне понимания:

– алгоритмы блочного шифрования;

– алгоритмы асимметричного шифрования;

– алгоритмы электронной цифровой подписи;

– алгоритмы идентификации и проверки подлинности;

уметь:

– шифровать данные классическими криптосистемами;

– защитить персональный компьютер от несанкционированного доступа;

– скрывать информацию на персональном компьютере;

– использовать программное обеспечение для шифрования/дешифрования файлов, частей или всего винчестера;

– создавать виртуальные зашифрованные диски.

Дисциплина «Защита компьютерной информации» рассчитана на 21 час занятий (17 часов лекций и 4 часа лабораторных занятий).

**ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН**

Дисциплины «Защита компьютерной информации»

|  |  |  |  |
| --- | --- | --- | --- |
| Раздел, тема | Количество часов | | |
| всего | в том числе | |
| на ла­бора­торные  работы | на практические  работы |
| Введение | 1 |  |  |
| Раздел 1. Особенности построения систем защиты информации в информационных системах различного типа | 16 | 4 |  |
| 1.1. Особенности защиты информации в информационно-справочных системах | 6 |  |  |
| Лабораторная работа №1  Защита баз данных средствами СУБД MS Access |  | 4 |  |
| 1.2. Особенности защиты информации в сложных корпоративных информационных системах | 2 |  |  |
| 1.3. Безопасность работы в сети Интернет | 6 |  |  |
| 1.4. Особенности защиты информации в системах электронного документооборота | 2 |  |  |
| **ИТОГО** | 17 | 4 |  |

**СОДЕРЖАНИЕ ПРОГРАММЫ**

|  |  |  |
| --- | --- | --- |
| Цель изучения темы | Содержание темы | Результат |
| Введение | | |
| Сформировать представление о содержании, целях и задачах учебной дисциплины, ее значении в подготовке специалистов среднего звена. | Содержание, цели и задачи учебной дисциплины «Защита компьютерной информации», ее значение в подготовке специалистов среднего звена. | Высказывает общее суждение о содержании, целях и задачах учебной дисциплины, ее значении в подготовке специалистов среднего звена. |
| Раздел 1. Особенности построения систем защиты информации  в информационных системах различного типа | | |
| Тема 1.1. Особенности защиты информации  в информационно-справочных системах | | |
| Сформировать представление о структуре и составе подсистемы защиты информации в информационно-справочных системах.  Дать понятие о методах и средствах защиты информации в системе управления базами данных (СУБД). | Назначение, состав и архитектура информационно-справочных систем. Угрозы информации, характерные для них. Модель потенциального нарушителя.  Структура и состав подсистемы защиты информации.  Методы и средства защиты информации в СУБД. | Называет угрозы информации, характерные для информационно-справочных систем.  Высказывает общее суждение о структуре и составе подсистемы защиты информации в информационно-справочных системах.  Излагает методы и средства защиты информации в СУБД. |
| Лабораторная работа № 1 | | |
| Сформировать навыки защиты ПО и базы данных средствами СУБД MS Access. | Защита баз данных средствами СУБД MS Access. | Реализует защиту ПО и базы данных средствами СУБД MS Access. |
| Тема 1.2. Особенности защиты информации  в сложных корпоративных информационных системах | | |
| Сформировать представление о структуре и составе подсистемы защиты информации в сложных корпоративных информационных системах. | Назначение, состав и архитектура сложных корпоративных информационных систем. Угрозы информации, характерные для них. Модель потенциального нарушителя. Структура и состав подсистемы защиты информации. | Называет угрозы информации, характерные для сложных корпоративных информационных систем. Высказывает общее суждение о структуре и составе подсистемы защиты информации в сложных корпоративных информационных систе­мах. |
| Тема 1.3. Безопасность работы в сети Интернет | | |
| Сформировать представ­ление о типовых удаленных атаках в Интернет и механизмах их реализации.  Дать понятие о типовых уязвимостях и методах обеспечения безопасности систем, входящих в состав глобальных сетей. | Типовые удаленные атаки в Интернет и механизмы их реализации. Типовые уязвимости, позволяющие реализовать удаленные атаки.  Обеспечение безопасности систем, входящих в состав глобальных сетей: межсетевые экраны, виртуальные частные сети.  Обеспечение безопасности электронной почты. | Высказывает общее суждение о типовых удаленных атаках в Интернет и механизмах их реализации.  Излагает сведения о типовых уязвимостях и методах обеспечения безопасности систем, входящих в состав глобальных сетей. |
| Тема 1.4. Особенности защиты информации  в системах электронного документооборота | | |
| Сформировать представление о структуре и составе подсистемы защиты информации в системах электронного документооборота. | Назначение, состав и архитектура систем электронного документооборота. Угрозы информации, характерные для них. Модель потенциального нарушителя.  Структура и состав подсистемы защиты информации. | Называет угрозы информации, характерные для систем электронного документооборота.  Высказывает общее суждение о структуре и составе подсистемы защиты информации в системах электронного документооборота. |

**ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ОСНАЩЕНИЯ ЛАБОРАТОРИИ**

|  |  |
| --- | --- |
| Наименование средств обучения | Количество |
| Технические средства обучения  Технические устройства\*  Компьютер  Комплект сетевого оборудования  Программное обеспечение  Операционная система Windows  Интегрированная среда разработки ПО для Microsoft Windows Visual Studio и язык программирования C  Обучающая программа по криптографии  Средства защиты (для учебных лабораторий)  Аптечка медицинская  Заземление  Огнетушитель  Оборудование помещения  Доска классная  Стол для преподавателя  Стол аудиторный  Стул  Шкаф книжный | 16  1  1  1  1  1  15  31  1 |

\* При отсутствии использовать специализированную аудиторию технических средств обучения.

**ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ**

**Основная**

Безбогов, А.А. Методы и средства защиты компьютерной информации / А.А.Безбогов, А.В.Яковлев, В.Н.Шамкин. Тамбов, 2006.

Макаренко, С.И. Информационная безопасность: учеб. пособие / С.И.Макаренко. Ставрополь, 2009.

Математические и компьютерные основы криптологии: учеб. пособие / Ю.С.Харин [и др.]. Минск, 2003.

Нестеров, С.А. Информационная безопасность и защита информации / С.А.Нестеров. СПб., 2009.

Основы криптографии: учеб. пособие / А.П.Алферов [и др.]. М., 2002.

Петров, А.А. Компьютерная безопасность. Криптографические методы защи­ты / А.А.Петров. М., 2000.

Тимошенко, А.А. Защита информации в специализированных информацион­нотелекоммуникационных системах / А.А.Тимошенко. Киев, 2010.

ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

**Дополнительная**

Казарин, О.В. Безопасность программного обеспечения компьютерных систем / О.В.Казарин. М., 2003.

Романец, Ю.Ф. Защита информации в компьютерных системах и сетях / Ю.Ф.Романец, П.А.Тимофеев, В.Ф.Шаньгин. М., 2001.

Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф.Шаньгин. М., 2011.

Щеглов, А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю.Щеглов. СПб., 2004.

**Нормативные правовые акты**

Конституция Республики Беларусь 1994 года (с изм. и доп., принятыми на республиканских референдумах 24.11.1996 и 17.10.2004 // Нац. реестр правовых актов Респ. Беларусь. 04.01.1999. № 1/0.

Кодекс Республики Беларусь об образовании от 13.01.2011 № 243-З // Нац. реестр правовых актов Респ. Беларусь. 17.01.2011. № 2/1795.

Единый тарифно-квалификационный справочник работ и профессий рабочих (ЕТКС): вып. 2: постановление М-ва труда Респ. Беларусь, 28 декабря 2000 г., № 160 // Нац. реестр правовых актов Респ. Беларусь. – 2012. – 8/25723.

**Технические нормативные правовые акты**

ISO/IEC 17799:2005 Информационная технология — Методы защиты — Практическое руководство для менеджмента информационной безопасности.

ISO/IES 27001:2013 Система обеспечения информационной безопасности.

**Стандарты**

Образовательный стандарт среднего специального образования по специальности 2-40 01 01 Программное обеспечение информационных технологий: ОС РБ 2-40 01 01-2014. – Утв. постановлением Министерства образования Респ. Беларусь № 54 от 28.04.2014 г. – Минск : М-во обр. Респ. Беларусь : УО РИПО, 2014. – 30с.

Приложение Д

**Фрагмент календарно-тематического плана**

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

ФИЛИАЛ БЕЛОРУССКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

«МИНСКИЙ РАДИОТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДАЮ |
|  |  | Зам. директора  по учебной работе  \_\_\_\_\_\_\_\_\_\_\_\_\_ Ф.С.Шумчик  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_г. |

**КАЛЕНДАРНО-ТЕМАТИЧЕСКИЙ ПЛАН**

(очная форма получения образования)

по учебной дисциплине «Защита компьютерной информации»

для групп № 844691, 944691 очной формы получения образования

Преподаватель Сабило Владимир Алексеевич

Составлен в соответствии с типовой учебной программой по учебной дисциплине «Защита компьютерной информации» профессионального компонента типового учебного плана по специальности 2-40 01 01 «Программное обеспечение информа­ционных технологий» для реализации образовательной программы среднего специального образования, обеспечивающей получение квалификации специалиста со средним специальным образованием, утвержденной постановлением Министерства образования Республики Беларусь 26.01.2017 № 6

Количество учебных часов по учебному плану 21

Из них:

на обзорные занятия 17

на лабораторные занятия (работы) 4

на практические занятия (работы) -

на курсовое проектирование -

Количество домашних контрольных работ -

Рассмотрен на заседании цикловой комиссии специальности «Программное обеспечение информационных технологий»

Протокол № \_\_\_\_\_ от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

Председатель цикловой комиссии \_\_\_\_\_\_\_\_\_\_\_\_ /Лазицкас Е.А./

Разработчик \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Сабило В.А./

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №№ учеб­ных заня­тий | №№ учебных групп | | | | | Наименование разделов, наименование тем по учебной программе, наименование тем отдельных учебных занятий | Количество учебных часов | Тип учебного занятия | Учебно-методическое обеспечение | Задание для самостоятельной работы учащимся | Литература  (печатная, электронная) | Примечание |
| 844691 | 944691 |  |  |  |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 1 |  |  |  |  |  | Введение | 1 |  |  |  |  |  |
|  |  |  |  |  |  | **Раздел 1. Особенности построения систем защиты информации в информационных системах различного типа** |  |  |  |  |  |  |
| 2,3,4 |  |  |  |  |  | 1.1. Особенности защиты информации в информационно-справочных системах | 6 | УЗФНЗ | Презентация «Защита информации в информационно-справочных системах» |  | [1, c.209-225] |  |
| 5,6 |  |  |  |  |  | ЛР №1 Защита баз данных средствами СУБД MS Access | 4 | ЛР |  |  |  |  |
| 7 |  |  |  |  |  | 1.2. Особенности защиты информации в сложных корпоративных информационных системах | 2 | УЗФНЗ | Презентация «Защита информации в сложных корпоративных информационных системах» |  | [1, c.225-227] |  |
| 8,9,  10 |  |  |  |  |  | 1.3. Безопасность работы в сети Интернет | 6 | УЗФНЗ | Международные стандарты информационной безопасности |  | [2, c.78-92] |  |
| 11 |  |  |  |  |  | 1.4. Особенности защиты информации в системах электронного документооборота | 2 | УЗФНЗ | Презентация по теме «Защита информации в системах электронного документооборота» |  | [1, c.157-181] |  |
|  |  |  |  |  |  | **Всего** | **21** |  |  |  |  |  |

Условные обозначения:

ЛР – лабораторная работа;

ПЗ – практическое занятие

ОКР – обязательная контрольная работа;

УЗФНЗ – учебное занятие формирования новых знаний;

УЗППЗ – учебное занятие практического применения знаний;

КУЗ – комбинированное учебное занятие;

УЗКЗ – учебное занятие контроля знаний.

**ЛИТЕРАТУРА**

|  |  |  |  |
| --- | --- | --- | --- |
| № №  п/п | Наименование | Автор | Издательство, год издания |
| Основная литература | | | |
| 1 | Защита информации в специализированных информационно-телекоммуникационных си­стемах | Тимошенко, А.А. | Киев, 2010 |
| 2 | Информационная безопасность компьютерных систем и сетей: учеб. пособие | Шаньгин, В.Ф. | М., 2011 |
| 3 | Информационная безопасность и защита ин­формации | Нестеров, С.А. | СПб., 2009 |
| 4 | Информационная безопасность: учеб. пособие | Макаренко, С.И. | Ставрополь, 2009 |
| 5 | Методы и средства защиты компьютерной информации | Безбогов, А.А. | Тамбов, 2006 |
| 6 | Защита компьютерной информации от несанкционированного доступа | Щеглов, А.Ю. | СПб., 2004 |

Приложение Е

**ПЛАН-КОНСПЕКТ лекционного занятия**

**«Особенности защиты информации в информационно-справочных системах» по дисциплине**

**«защита компьютерной информации»**

**направления специальности 2-40 01 01 «программное**

**обеспечение информационных технологий»**

Дисциплина: Защита компьютерной информации

Тема учебного занятия: «**Особенности защиты информации в информационно-справочных системах» (6 часов)**

**Цели лекции**: изучить назначение, состав и архитектура информационно-справочных систем. Угрозы информации, характерные для них; модель потенциального нарушителя; структуру и состав подсистемы защиты информации; методы и средства защиты информации в СУБД.

**Форма проведения учебного занятия:** лекция

**Задачи лекции**:

1. обучающая:
2. сформировать представление о структуре и составе подсистемы защиты информации в информационно-справочных системах;
3. сформировать понятие о методах и средствах защиты информации в системе управления базами данных (СУБД);
4. сформировать знания о структуре и составе подсистемы защиты информации, о модели потенциального нарушителя, об угрозах информации;
5. воспитательная:
6. способствовать воспитанию усидчивости, организованности, дисциплинированности;
7. развивающая:
8. способствовать развитию умений учащихся обобщать полученные знания, проводить анализ, синтез, сравнения, делать необходимые выводы.

**План лекции:**

1. Назначение, состав и архитектура информационно-справочных систем.
2. Угрозы информации, характерные для ИСС.
3. Модель потенциального нарушителя в ИСС.
4. Особенности построения систем защиты информации в ИСС.
5. Методы и средства защиты информации в СУБД.
6. Заключение.
7. Вопросы для контроля знаний.

**Используемые средства обучения:** мультимедийная презентация.

**Конспект лекции:**

**1. Назначение, состав и архитектура информационно-справочных систем**

Информационно-справочные системы (ИСС) — системы, предназначенные для обеспечения доступа пользователей к хранилищам общедоступной справочной информации и реализации с этой целью необходимых функций по поиску требуемой информации, передаче ее поль­зователю и представлению в удобном для пользователя виде.

Как правило, ИСС включает в себя подсистему администрирования ИСС и подсистему обеспечения доступа к информации ИСС (подсистему публикации).

Подсистема администрирования ИСС предназначена для реализации функций, связанных с управлением структурой информационного хранилища ИСС, его информационным наполнением (вводом, актуализацией информа­ции), управлением регламентом и правилами доступа пользователей к информационным ресурсам ИСС.

Подсистема обеспечения доступа к информации ИСС (подсистема публикации) предназначена для обеспечения доступа конечных пользователей к ресурсам ИСС через сеть передачи данных и реализации бизнес-логики системы по поиску и представлению пользователям необходимой информации.

На сегодняшний день большинство ИСС реализовано с использованием Web-технологий (представление информации в виде статически или динамически генерируемых HTML (XML) – страниц, передача ее с использованием протокола HTTP).

Современные ИСС относятся, как правило, к системам распределенной двухуровневой или трехуровневой архитектуры.

Основными компонентами подсистемы обеспечения доступа к информации ИСС с двухуровневой архитектурой являются:

* web-сервер — сервер, обеспечивающий пользователям сети Internet (или любой другой сети со стеком протоколов TCP/IP) доступ к статически сгенерированным HTML (XML)-страницам, связанным между собой гипертекстовыми ссылками (по протоколу HTTP);
* web-клиент — программа, используемая для доступа к Web-серверу ИСС (по протоколу HTTP) с целью получения, форматирования и просмотра сгенерированных на сервере HTML (XML) страниц.

Основными компонентами подсистемы обеспечения доступа к информации ИСС с трехуровневой архитектурой являются:

* сервер СУБД — сервер, обеспечивающий управление хранилищем данных справочной и служебной информации ИСС;
* сервер приложений/Web-сервер — сервер, реализующий бизнес-логику системы (поиск информации в СУБД на основе запроса пользователя, динамическую генерацию HTML (XML)страниц на основе выбранной информации) и обеспечивающий пользователям сети Internet (или любой другой сети со стеком протоколов TCP/IP) доступ к динамически сгенерированным HTML (XML)-страницам, связанным между собой гипертекстовыми ссылками (по протоколу HTTP);
* web-клиент — программа, используемая для доступа к Web-серверу ИСС (по протоколу HTTP) с целью получения, форматирования и просмотра сгенерированных на сервере HTML (XML)страниц.

Основными компонентами подсистемы администрирования ИСС с двухуровневой архитектурой являются:

* сервер приложений — сервер, обеспечивающий возможность упол­номоченным пользователям (администраторам) получать доступ к статически сгенерированным HTML (XML)-страницам, содержащим справочную информацию, связанным между собой гипертекстовыми ссылками (по соответствующему протоколу), а также служебным (конфигурационным) данным ИСС. Например, в простейшем случае в качестве такового может использоваться FTP-сервер;
* клиент сервера приложений — программа, используемая для доступа к серверу приложений подсистемы администрирования ИСС (по соответствующему протоколу) с целью обеспечения возможности администратору ИСС выполнения соответствующих функций по управлению ИСС. Например, в простейшем случае в качестве такового может использоваться FTP-клиент.

Основными компонентами подсистемы администрирования ИСС с трехуровневой архитектурой являются:

* сервер СУБД — сервер, обеспечивающий управление хранилищем данных справочной и служебной информации ИСС;
* сервер приложений — сервер, обеспечивающее возможность уполномоченным пользователям (администраторам) получать доступ к хранилищу базы данных справочной и служебной информации ИСС по соответствующему протоколу (например, протоколу SOAP) и реализации необходимых функций по управлению ИСС;
* клиент сервера приложений — программа, используемая для доступа к серверу приложений подсистемы администрирования ИСС (по соответствующему протоколу) с целью обеспечения возможности администратору ИСС выполнения соответствующих функций по управлению ИСС.

В общем случае в состав подсистем ИСС могут также входить следующие типовые компоненты ИТС: файловый сервер ЛВС, рабочая станция локальной вычислительной сети (ЛВС), PROXY-сервер, устройства коммутации, устройства маршрутизации, каналы передачи данных.

**2. Угрозы информации, характерные для ИСС**

Основными информационными ресурсами, подлежащими защите в ИСС (информационными активами), являются:

* информационные объекты, содержащие технологическую информацию ИСС;
* информационные объекты, содержащие общедоступную информацию ИСС.

Особенности ИСС как объекта защиты:

* технологические особенности работы пользователей с общедоступной информацией Web страницы определяются особенностями системного и функционального ПО, в частности Internet-браузеров, которыми они пользуются;
* технологические особенности работы пользователей с технологиче­ской информацией ИСС определяются архитектурой ИСС, способами обработки и передачи технологической информации между компонентами ИСС и способами осуществления доступа к ней;
* возможны следующие способы осуществления доступа к технологической информации ИСС (в т.ч. передачи данных для актуализации общедоступной информации): с рабочей станции подсистемы администрирования, размещенной в пределах одной ЛВС с Web-сервером и другими компонентами ИСС (на территории собственника Web-страницы или на территории оператора); с рабочей станции подсистемы администрирования, размещенной за пределами ЛВС оператора, в которой находятся Web-сервер и другие компоненты ИСС (размещенной, например на территории собственника Web-страницы), взаимодействие внутри подсистемы администрирования при этом осуществляется по каналам сети передачи данных.

Информационные объекты, содержащие технологическую информацию ИСС, могут быть представлены в виде:

* структурированных и неструктурированных записей БД (сервер СУБД, сервер приложений подсистемы администрирования);
* структурированных и неструктурированных файлов (ФС ЛВС);
* структурированных и неструктурированных сообщений, передаваемых по сети передачи данных (в случае, когда взаимодействие внутри подсистемы администрирования осуществляется по каналам сети передачи данных).

В штатном режиме функционирования ИСС к данным информационным объектам невозможен разделяемый доступ с целью просмотра и модификации.

Информационные объекты, содержащие общедоступную информацию ИСС, могут быть представлены в виде:

* структурированных и неструктурированных записей БД (сервер СУБД, сервер приложений подсистемы обеспечения доступа к информации ИСС);
* структурированных и неструктурированных сообщений в виде HTML(XML)- страниц (Web-сервер);
* структурированных и неструктурированных файлов HTML(XML)-страниц (ФС ЛВС).

В штатном режиме функционирования ИСС к данным информационным объектам возможен разделяемый доступ с целью просмотра.

Наиболее значимыми (с точки зрения наносимого информационным активам ущерба) типами угроз информации в ИСС являются угрозы с целью нарушения:

* конфиденциальности информации по отношению к информационным объектам, содержащим технологическую информацию ИСС, путем несанкционированного ознакомления;
* целостности информации по отношению к информационным объек­там, содержащим технологическую информацию ИСС и к информационным объектам, содержащим общедоступную информацию ИСС, путем несанкци­онированной модификации;
* доступности разделяемых ресурсов Web-сервера/сервера приложений (реализующего бизнес логику), ФС, сервера СУБД (реализующего функции управления хранилищем данных ИСС) при доступе пользователей к информационным объектам, содержащим общедоступную информацию ИСС.

**3. Модель потенциального нарушителя в ИСС**

В качестве потенциального нарушителя в ИСС должны рассматриваться:

* любой сотрудник организации-владельца Web-страницы или организации-оператора, на ресурсах которого функционирует Web-страница;
* сотрудник организации-владельца Web-страницы, не уполномоченный выполнять функции администрирования Web-страницей, функционирующей на ресурсах оператора;
* любой внешний по отношению к оператору или к организации-владельцу Web-страницы, пользователь ИТС (в том числе и осуществляющий доступ к общедоступной информации).

Сотрудник организации-владельца Web-страницы или организации-оператора, на ресурсах которого функционирует Web-страница:

* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к обрабатываемым и сохраняемым в ИСС с использованием разделяемых ресурсов (сервер приложений подсистемы администрирования, сервер СУБД, ФС) информационным объектам, содержащим технологическую информацию ИСС (с целью их просмотра или модификации);
* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к обрабатываемым и сохраняемым в ИСС с использованием разделяемых ресурсов (сервер приложений подсистемы администрирования, сервер приложений подсистемы обеспечения доступа / Web-сервер, сервер СУБД, ФС) информационным объектам, содержащим общедоступную информацию ИСС (с целью их модификации или удаления);
* с использованием штатных и нештатных средств может влиять на работоспособность разделяемых ресурсов ИСС, (сервер приложений подсистемы обеспечения доступа / Web-сервер, ФС, сервера СУБД), активного сетевого оборудования.

Сотрудник организации-владельца Web-страницы, не уполномоченный выполнять функции администрирования Web-страницы, функционирующей на ресурсах оператора, или внешний по отношению к оператору или к организации-владельцу Web-страницы, пользователь информационно-телекоммуникационной сети (ИТС):

* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к обрабатываемым и сохраняемым в ИСС с использованием разделяемых ресурсов, взаимодействующих с сетью переда­чи данных (сервер приложений подсистемы администрирования, сервер СУБД, ФС) информационным объектам, содержащим технологическую информацию ИСС (с целью их просмотра или модификации);
* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к информационным объектам, содержащим технологическую информацию ИСС, передаваемым между компонентами подсистемы администрирования ИСС по каналам сети передачи данных (с целью их просмотра, модификации или удаления);
* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к обрабатываемым и сохраняемым в ИСС с использованием разделяемых ресурсов, взаимодействующих с сетью передачи данных (сервер приложений подсистемы администрирования, сервер приложений подсистемы обеспечения доступа / Web-сервер, сервер СУБД, файловая система (ФС)) информационным объектам, содержащим общедоступную информацию ИСС (с целью их модификации или удаления);
* с использованием штатных и нештатных средств может влиять на работоспособность разделяемых ресурсов ИСС, взаимодействующих с сетью передачи данных (сервер приложений подсистемы обеспечения доступа / Web-сервер, ФС, сервер СУБД), активного сетевого оборудования и оборудования сети передачи данных.

Таким образом, потенциальный нарушитель имеет возможность реализации всех типов угроз (конфиденциальности, целостности и доступности) с использованием штатных средств ИСС, штатных и нештатных средств ОС, используемых ФС, штатных и нештатных средств серверов СУБД, штатных и нештатных средств серверов приложений, штатных и нештатных средств управления активным сетевым оборудованием и оборудованием сети передачи данных.

**4. Особенности построения систем защиты информации в ИСС**

Функциональная спецификация комплексов средств защиты (КСЗ) системы защиты информации в ИСС для технологии Т1 (Web-сервер и рабочие станции подсистемы администрирования размещаются в пределах ЛВС на территории собственника Web-страницы или на территории оператора):

* КА-2 — базовая административная конфиденциальность;
* ЦА-1 — минимальная административная целостность;
* ЦО-1 — ограниченный откат;
* ДР-1 — квоты;
* ДВ-1 — ручное восстановление;
* НР-2 — защищенный журнал;
* НО-1 — выделение администратора;
* НЦ-1 — КСЗ с контролем целостности;
* НТ-1 — самотестирование по запросу;
* НИ-2 — одиночная идентификация и аутентификация;
* НК-1 — достоверный канал.

Функциональная спецификация КСЗ системы защиты информации в ИСС для технологии Т2 (Web-сервер размещается на территории оператора, рабочие станции подсистемы администрирования размещаются на террито­рии собственника Web-страницы, взаимодействие внутри подсистемы адми­нистрирования осуществляется по каналам сети передачи данных):

* КА-2 — базовая административная конфиденциальность;
* КВ-1 — минимальная конфиденциальность при обмене;
* ЦА-1 — минимальная административная целостность;
* ЦО-1 — ограниченный откат;
* ЦВ-1 — минимальная целостность при обмене;
* ДР-1 — квоты;
* ДВ-1 — ручное восстановление;
* НР-2 — защищенный журнал;
* НО-1 — выделение администратора;
* НЦ-1 — КСЗ с контролем целостности;
* НТ-1 — самотестирование по запросу;
* НИ-2 — одиночная идентификация и аутентификация;
* НК-1 — достоверный канал;
* НВ-1 — аутентификация узла.

Рассмотрим несколько из них.

КА-2 — базовая административная конфиденциальность

Политика данной услуги должна быть реализована относительно:

* информационных объектов, содержащих технологическую информацию ИСС в виде: структурированных и неструктурированных записей БД (сервер СУБД, сервер приложений подсистемы администрирования); структурированных и неструктурированных файлов (ФС ЛВС);
* программных средств ИСС в виде файлов.

Политика услуги должна обеспечивать предотвращение реализации угроз конфиденциальности путем несанкционированного доступа к файлам данных и записям БД (предотвращая возможность их несанкционированного чтения), а также к файлам программных средств (предотвращая возможность их несанкционированного запуска).

Средства реализации услуги должны функционировать в таких компонентах ИТС: ФС ЛВС; сервер СУБД; сервер приложений подсистемы администрирования.

Для реализации услуги должны использоваться такие механизмы: управление доступом (на основе списков управления доступом).

КВ-1 — минимальная конфиденциальность при обмене

Политика данной услуги должна быть реализована относительно:

информационных объектов, содержащих технологическую информацию ИСС в виде: структурированных и неструктурированных сообщений, передаваемых по каналам сети передачи данных;

Политика услуги должна обеспечивать предотвращение реализации угроз конфиденциальности путем перехвата сообщений, передаваемых по каналам сети передачи данных (предотвращая возможность ознакомления с их содержимым).

Средства реализации услуги должны функционировать в таких компонентах ИТС: серверах приложений подсистемы администрирования ИСС; клиентах серверов приложений подсистемы администрирования ИСС.

Для реализации услуги должны использоваться такие механизмы: шифрование (симметричное).

ЦА-1 — минимальная административная целостность

Политика данной услуги должна быть реализована относительно:

* информационных объектов, содержащих технологическую информацию ИСС в виде: структурированных и неструктурированных записей БД (сервер СУБД, сервер приложений подсистемы администрирования); структурированных и неструктурированных файлов (ФС ЛВС);
* информационных объектов, содержащих общедоступную информацию ИСС в виде: структурированных и неструктурированных записей БД (сервер СУБД, сервер приложений подсистемы администрирования, сервер приложений подсистемы обеспечения доступа к информации ИСС); структурированных и неструктурированных сообщений в виде HTML(XML)-страниц (Web-сервер); структурированных и неструктурированных файлов HTML(XML)-страниц (ФС ЛВС);
* программных средств ИСС в виде файлов.

Политика услуги должна обеспечивать предотвращение реализации угроз целостности путем несанкционированного доступа к файлам данных и записям БД, а также к файлам программных средств (предотвращая возможность их несанкционированного создания, модификации или удаления).

Средства реализации услуги должны функционировать в таких компонентах ИТС: ФС ЛВС; сервер СУБД; сервер приложений подсистемы администрирования; сервер приложений подсистемы обеспечения доступа к информации; Web-сервер.

Для реализации услуги должны использоваться такие механизмы: управление доступом (на основе списков управления доступом).

ЦО-1 — ограниченный откат

Политика данной услуги должна быть реализована относительно:

* информационных объектов, содержащих технологическую информацию ИСС в виде: структурированных и неструктурированных записей БД (сервер СУБД, сервер приложений подсистемы администрирования); структурированных и неструктурированных файлов (ФС ЛВС);
* информационных объектов, содержащих общедоступную информацию ИСС в виде: структурированных и неструктурированных записей БД (сервер СУБД, сервер приложений подсистемы администрирования); структурированных и неструктурированных файлов HTML(XML)- страниц (ФС ЛВС);
* программных средств ИСС в виде файлов.

Политика данной услуги должна обеспечивать предотвращение угроз нарушения целостности путем обеспечения возврата информационных объ­ектов, целостность которых была нарушена, в предыдущее известное состоя­ние.

Средства реализации услуги должны функционировать в таких компонентах ИТС: ФС ЛВС; сервер СУБД; сервер приложений подсистемы администрирования. Для реализации услуги должны использоваться такие механизмы: обеспечение целостности путем репликации данных; обеспечение целостности путем повтора сообщений; контроль целостности по ККЦ; - контроль целостности по контексту.

ЦВ-1 — минимальная целостность при обмене

Политика данной услуги должна быть реализована относительно:

* информационных объектов, содержащих технологическую информацию ИСС в виде: структурированных и неструктурированных сообщений, передаваемых по сети передачи данных.

Политика услуги должна обеспечивать предотвращение реализации угроз целостности путем искажения сообщений, передаваемых по каналам сети передачи данных (обнаруживая факты их модификации).

Средства реализации услуги должны функционировать в таких компонентах ИТС: серверах приложений подсистемы администрирования ИСС; клиентах серверов приложений подсистемы администрирования ИСС.

Для реализации услуги должны использоваться такие механизмы: контроль целостности по ККЦ.

ДР-1 — квоты

Политика данной услуги должна быть реализована относительно:

* информационных объектов, содержащих технологическую информацию ИСС в виде: структурированных и неструктурированных записей БД (сервер СУБД, сервер приложений подсистемы администрирования); структурированных и неструктурированных файлов (ФС ЛВС);
* информационных объектов, содержащих общедоступную информацию ИСС в виде: структурированных и неструктурированных записей БД (сервер СУБД, сервер приложений подсистемы обеспечения доступа к информации ИСС); структурированных и неструктурированных сообщений в виде HTML(XML)- страниц (Web-сервер); структурированных и неструктурированных файлов HTML(XML)- страниц (ФС ЛВС).

Политика услуги должна обеспечивать предотвращение реализации угроз доступности путем захвата чрезмерного объема ресурсов серверов ФС ЛВС, сервера СУБД, Web-сервера и серверов приложений.

Средства реализации услуги должны функционировать в таких компонентах ИТС: ФС ЛВС (по отношению к выделяемому дисковому пространству); сервер СУБД (по отношению к выделяемому объему таблиц БД); сервер приложений подсистемы администрирования; сервер приложений подсистемы обеспечения доступа (по отношению к выделяемым объемам вычислительных ресурсов- процессорному времени, оперативной памяти); Web-сервер (по отношению к выделяемым объемам вычислительных ресурсов- процессорному времени, оперативной памяти, количеству устанавливаемых соединений).

Для реализации услуги должны использоваться такие механизмы: управление доступом (на основе списков управления доступом или на основе меток) с контролем установленных ограничений.

ДВ-1 — ручное восстановление

Должна быть реализована относительно всех компонентов ИТС, входящих в состав ИСС, через которые обеспечивается доступ к разделяемым ресурсам: ФС ЛВС; РС ЛВС (используемых подсистемой администрирования); сервер СУБД; сервер приложений подсистемы администрирования; - клиент сервера приложений подсистемы администрирования; сервер приложений подсистемы обеспечения доступа; Web-сервер; средства маршрутизации пакетов сетевых протоколов; средства коммутации пакетов сетевых протоколов; канал передачи данных.

Политика услуги должна обеспечивать минимизацию последствий реализации угроз доступности, приводящих к нарушению работоспособности компонентов ИТС.

Для реализации услуги должны использоваться такие механизмы: резервирование программных средств и информации с возможностью ручного восстановления.

НР-2 — защищенный журнал

Должна быть реализована относительно всех защищенных объектов во всех видах представления.

Средства реализации услуги должны функционировать в таких компонентах ИТС: ФС ЛВС; РС ЛВС (используемых подсистемой администрирования); сервер СУБД; сервер приложений подсистемы администрирования; клиент сервера приложений подсистемы администрирования; сервер приложений подсистемы обеспечения доступа; Web-сервер; средства маршрутизации пакетов сетевых протоколов; средства коммутации пакетов сетевых протоколов.

Политика услуги должна обеспечивать возможность аудита действий пользователей и является необходимой для корректной реализации остальных услуг.

Для реализации услуги должны использоваться такие механизмы: регистрация и аудит.

**5. Методы и средства защиты информации в СУБД**

Система управления базами данных (СУБД) — специализированное программное обеспечение, обеспечивающее доступ к базе данных как к совокупности её структурных единиц.

В настоящее время практически ни одна современная организация не обходится без использования баз данных в своей деятельности. База данных (БД) — это наиболее значимый и ценный актив для любой компании. Поскольку в БД может храниться очень деликатная или конфиденциальная информация, необходимо очень серьезно относиться к ее защите. Любые сбои в работе СУБД и баз данных могут привести к катастрофическим по­следствиям.

К основным средствам защиты информации относят следующие:

* парольная защита;
* защита полей и записей таблиц БД.
* установление прав доступа к объектам БД;
* шифрование данных и программ.

Защита БД производится на двух уровнях:

* на уровне пароля;
* на уровне пользователя (защита учетных записей пользователей и идентифицированных объектов).

Безопасная система авторизации и регистрации является одним из важ­нейших элементов при создании проекта. Один из возможных способов — это создание системы регистрации с помощью PHP и MySQL.

**6. Заключение**

Информационно-справочные системы (ИСС) – системы, предназначенные для обеспечения доступа пользователей к хранилищам общедоступной справочной информации и реализации с этой целью необходимых функций по поиску требуемой информации, передаче ее пользователю и представлению в удобном для пользователя виде.

На сегодняшний день большинство ИСС реализовано с использованием Web-технологий (представление информации в виде статически или динамически генерируемых HTML (XML) — страниц, передача ее с использованием протокола HTTP).

Основными компонентами подсистемы администрирования ИСС с двухуровневой архитектурой являются: сервер приложений, клиент сервера приложений.

Основными компонентами подсистемы администрирования ИСС с трехуровневой архитектурой являются: сервер СУБД, сервер приложений, клиент сервера приложений.

В общем случае в состав подсистем ИСС могут также входить следующие типовые компоненты ИТС: файловый сервер ЛВС, рабочая станция локальной вычислительной сети (ЛВС), PROXY-сервер, устройства коммутации, устройства маршрутизации, каналы передачи данных.

Основными информационными ресурсами, подлежащими защите в ИСС (информационными активами), являются:

* информационные объекты, содержащие технологическую информацию ИСС;
* информационные объекты, содержащие общедоступную информацию ИСС.

Система управления базами данных (СУБД) — специализированное программное обеспечение, обеспечивающее доступ к базе данных как к совокупности её структурных единиц.

**7.** **Вопросы для контроля знаний**

1. Что такое ИИС?
2. Каким образом реализуется ИИС в настоящее время?
3. Назовите архитектуры ИСС.
4. Перечислите компоненты подсистем администрирования ИСС каждой архитектуры.
5. Какие компоненты ИТС являются типовыми?
6. Что такое СУБД?
7. Перечислите основные средства защиты информации БД.
8. Перечислите уровни защиты СУБД.

**Рекомундуемый список литературы:**

[1] Тимошенко, А.А. Защита информации в специализированных информационно-телекоммуникационных системах / А.А.Тимошенко. Киев, 2010.

[2] Методы защиты и безопасность базы данных // Новаинфо [Электронный ресурс]. – Режим доступа: https://novainfo.ru/article/13078 – Дата доступа: 28.05.2020.

[3] База данных и СУБД: основные понятия и определения // Patches [Электронный ресурс]. – Режим доступа: https://oracle-patches.com/db/3205-база-данных-и-субд-основные-понятия. – Дата доступа: 28.05.2020.

Преподаватель В.А. Сабило

Приложение Ж

**ПЛАН-КОНСПЕКТ лекционного занятия**

**«Особенности защиты информации в сложных**

**корпоративных информационных системах»**

**по дисциплине «защита компьютерной информации»**

**направления специальности 2-40 01 01 «программное**

**обеспечение информационных технологий»**

Дисциплина: Защита компьютерной информации

Тема учебного занятия: «**Особенности защиты информации в сложных корпоратив­ных информационных системах» (2 часа)**

**Цели лекции**: изучить назначение, состав и архитектура сложных корпоративных информа­ционных систем; угрозы информации, характерные для них; модель потенциального нарушителя; структуры и состав подсистемы защиты информации.

**Форма проведения учебного занятия:** лекция

**Задачи лекции**:

1. обучающая:
2. сформировать представление о структуре и составе подсистемы защиты информации в сложных корпоративных информационных системах;
3. сформировать знания о назначении, составе и архитектуре сложных корпоративных информационных систем;
4. сформировать знания о структуре и составе подсистемы защиты информации, о модели потенциального нарушителя, об угрозах информации;
5. воспитательная:
6. способствовать воспитанию усидчивости, организованности, дисциплинированности;
7. развивающая:
8. способствовать развитию умений учащихся обобщать полученные знания, проводить анализ, синтез, сравнения, делать необходимые выводы.

**План лекции:**

1. Назначение, состав и архитектура сложных корпоративных информационных систем.
2. Угрозы информации, характерные для сложных корпоративных ИТС. Модель потенциального нарушителя в сложных корпоративных ИТС.
3. Особенности построения систем защиты информации в сложных корпоративных ИТС.
4. Заключение.
5. Вопросы для контроля знаний.

**Используемые средства обучения:** мультимедийная презентация.

**Конспект лекции:**

**1. Назначение, состав и архитектура сложных корпоративных**

**информационных систем**

Сложная корпоративная ИТС — ИТС, построенная на основе РВС и предназначенная для автоматизации разнородных бизнес-процедур крупного территориально-распределенного предприятия или организации.

В состав сложной корпоративной ИТС в качестве прикладных подсистем могут входить специализированные ИТС любого из рассмотренных ранее типов, например, системы ЭП; системы ЭДО; элементы АБС, например, система «Клиент-банк»; ИСС, а также любые другие прикладные подсистемы, предназначенные для автоматизации различных бизнес-процедур.

В составе сложной корпоративной ИТС могут использоваться любые типовые компоненты ИТС: каналы передачи данных (обмена данными); устройства коммутации пакетов; устройства маршрутизации пакетов; ФС ЛВС; рабочие станции ЛВС; серверы приложений общего назначения; клиенты серверов приложений общего назначения; серверы СУБД; клиенты СУБД; серверы системы ЭП; клиенты системы ЭП; Web-серверы; Proxy-серверы.

Прикладные подсистемы, входящие в состав сложной корпоративной ИТС, могут относиться к архитектуре ИТС любого типа: локализованной файл-серверной; локализованной и распределенной двухуровневой клиент-серверной; локализованной и распределенной трехуровневой клиент-серверной.

**2. Угрозы информации, характерные для сложных корпоративных ИТС.**

**Модель потенциального нарушителя в сложных корпоративных ИТС**

С учетом структуры и состава сложных корпоративных ИТС, а также различного характера обрабатываемой в различных подсистемах информации, требующие защиты информационные ресурсы (информационные активы) и модель потенциального нарушителя должны определяться для каждой прикладной подсистемы отдельно (по аналогии с рассмотренными ранее для ИТС различного назначения). Совокупная модель потенциального нарушителя должна объединять возможности нарушителей, характерные для каждой прикладной подсистемы.

При определении потенциальных угроз информации должны быть учтены следующие особенности сложных корпоративных ИТС, влияющие на обеспечение защищенности обрабатываемой информации (с точки зрения использования различных способов реализации угроз информации):

* территориальная распределенность;
* распределенность информационных ресурсов внутри ИТС;
* интеграция с распределенными сетями;
* неоднородность с точки зрения функционального назначения входящих в состав ИТС компонентов (файловые серверы, серверы приложений (HTTP, FTP и т.п.), серверы СУБД, рабочие станции, активное сетевое оборудование — устройства маршрутизации, устройства коммутации и т.п.);
* неоднородность с точки зрения используемых ОС и прикладных программных средств;
* распределение обязанностей по администрированию ОС, прикладных систем и других компонентов ИТС между различными лицами.

Указанные особенности приводят к тому, что в сложных корпоратив­ных ИТС достаточно высока вероятность реализации угроз информации всех типов (конфиденциальности, целостности и доступности) различного харак­тера и природы:

* объективных, например, вызванными изменением условий физической среды или отказом элементов ИТС;
* субъективных, например, ошибок пользователей или действия нарушителей;
* случайных (неумышленных);
* преднамеренных, т.е. являющихся результатом намеренных действий пользователей ИТС или сторонних лиц по реализации различных угроз информации;
* прямых — напрямую связанными с нарушением установленных в ИТС ПРД;
* непрямых (косвенных) — таких, которые напрямую не приводят к нарушению установленных в ИТС ПРД, но в некоторых случаях могут привести к нарушению принятой политики безопасности (ПБ);
* внутренних, вызванных действиями пользователей ИТС или другими внутренними факторами;
* внешних, вызванных действиями сторонних лиц или внешними по отношению к ККС обстоятельствами.

Важно помнить, что, по различным данным, до 80 процентов нарушений в ИТС различного типа является внутренними.

**3. Особенности построения систем защиты информации**

**в сложных корпоративных ИТС**

Особенности сложных корпоративных ИТС, влияющие на обеспечение защищенности обрабатываемой информации (с точки зрения влияния на структуру и состав СЗИ):

* территориальная распределенность;
* распределенность информационных ресурсов внутри ИТС;
* интеграция с распределенными сетями;
* неоднородность с точки зрения функционального назначения входящих в состав ИТС компонентов (файловые серверы, серверы приложений (HTTP, FTP и т.п.), серверы СУБД, рабочие станции, активное сетевое оборудование — устройства маршрутизации, устройства коммутации и т.п.);
* неоднородность с точки зрения используемых ОС и прикладных программных средств;
* реализация в большинстве используемых компонентов тех или иных стандартных (штатных) средств защиты, реализующих те или иные механизмы защиты информации (те или иные функциональные услуги безопасности) и возможность использования данных средств в КСЗ;
* распределение обязанностей по администрированию ОС, прикладных систем и других компонентов ИТС между различными лицами;
* отсутствие единых средств управления средствами защиты и средств контроля функционирования средств защиты информации.

Функциональный профиль защищенности информации в сложных кор­поративных ИТС должен разрабатываться с учетом особенностей политики реализации функциональных услуг безопасности при реализации КСЗ информации в каждой прикладной подсистеме. Важным является использование централизованных средств администрирования средств защиты и централизованных средств контроля соблюдения политики безопасности.

**4. Заключение**

Сложная корпоративная ИТС – ИТС, построенная на основе РВС и предназначенная для автоматизации разнородных бизнес-процедур крупного территориально-распределенного предприятия или организации.

В состав сложной корпоративной ИТС в качестве прикладных подсистем могут входить специализированные ИТС любого из рассмотренных ранее типов, например, системы ЭП; системы ЭДО; элементы АБС, например, система «Клиент-банк»; ИСС, а также любые другие прикладные подсистемы, предназначенные для автоматизации различных бизнес-процедур.

В составе сложной корпоративной ИТС могут использоваться любые типовые компоненты ИТС: каналы передачи данных (обмена данными); устройства коммутации пакетов; устройства маршрутизации пакетов; ФС ЛВС; рабочие станции ЛВС; серверы приложений общего назначения; клиенты серверов приложений общего назначения; серверы СУБД; клиенты СУБД; серверы системы ЭП; клиенты системы ЭП; Web-серверы; Proxy-серверы.

**5. Вопросы для контроля знаний**

1. Что такое сложная корпоративная ИТС?
2. Что может входить в состав сложной корпоративной ИТС?
3. Перечислите компоненты подсистем администрирования ИСС каждой архитектуры.
4. К каким архитектурам ИТС могут относиться прикладные подсистемы?
5. Перечислите особенности, учитываемые при определении потенциальных угроз информации.
6. Перечислите основные типы угроз информации.

**Рекомундуемый список литературы:**

[1] Тимошенко, А.А. Защита информации в специализированных информационно-телекоммуникационных системах / А.А.Тимошенко. Киев, 2010.

[2] Нестеров, С.А. Информационная безопасность и защита информации / С.А.Нестеров. СПб., 2009.

Преподаватель В.А. Сабило

Приложение И

**ПЛАН-КОНСПЕКТ лекционного занятия**

**«Особенности защиты информации**

**в системах электронного документооборота»**

**по дисциплине «защита компьютерной информации»**

**направления специальности 2-40 01 01 «программное**

**обеспечение информационных технологий»**

Дисциплина: Защита компьютерной информации

Тема учебного занятия: «**Особенности защиты информации в системах электронно­го документооборота» (2 часа)**

**Цель лекции**: изучить назначение, состав и архитектура систем электронного документо­оборота; угрозы информации, характерные для них; модель потенциального нарушителя; структуру и состав подсистемы защиты информации.

**Форма проведения учебного занятия:** лекция

**Задачи лекции**:

1. обучающая:
2. сформировать представление о структуре и составе подсистемы защиты информации в системах электронного документооборота;
3. сформировать знания о назначении, составе и архитектуре систем электронного документооборота;
4. сформировать знания о структуре и составе подсистемы защиты информации, о модели потенциального нарушителя, об угрозах информации;
5. воспитательная:
6. способствовать воспитанию усидчивости, организованности, дисциплинированности;
7. развивающая:
8. способствовать развитию умений учащихся обобщать полученные знания, проводить анализ, синтез, сравнения, делать необходимые выводы.

**План лекции:**

1. Назначение, состав и архитектура систем электронного документооборота.
2. Угрозы информации, характерные для систем электронного документооборота.
3. Модель потенциального нарушителя в системе электронного документооборота.
4. Особенности построения систем защиты информации в системе электронного документооборота.
5. Заключение.
6. Вопросы для контроля знаний.

**Используемые средства обучения:** мультимедийная презентация.

**Конспект лекции:**

**1. Назначение, состав и архитектура систем**

**электронного документооборота**

Системы электронного документооборота (СЭД) — системы, предназначенные для автоматизации процессов создания, учета и обработки документов в электронном виде (электронных документов).

Все СЭД содержат обязательные типовые компоненты: хранилище карточек (атрибутов) документов; хранилище документов; компоненты, реализующие бизнес-логику системы.

Хранилище атрибутов документов - предназначено для хранения «карточки» — набора полей, характеризующих документ.

Хранилище документов - предназначено для хранения непосредственного содержимого документа.

Компоненты, реализующие бизнес-логику системы — обеспечивают непосредственную реализацию функций СЭД. Среди основных функций, реализуемых данными компонентами, можно выделить:

* управление документами в хранилище. Включает процедуры добавления и изъятия документов, сохранения версий, передачи на хранение в архив, поддержания архива и т.д.;
* поиск документов. Состоит из поиска по атрибутам, визуального поиска по различным деревьям, в которые уложены документы, поиска по полному тексту, смыслового поиска и т.д.;
* маршрутизация и контроль исполнения. Обеспечивает доставку документов в рамках бизнеспроцедур в организации. Маршруты документов могут быть гибкими и жесткими. В случае гибкой маршрутизации следующий получатель документа определяется сотрудником, в ведении которого документ находится в данный момент. В случае жесткой маршрутизации путь прохождения документов определяется заранее на основе некоторой логики. Фактически, маршрут определяется в терминах пути прохождения и временных интервалов на исполнение документа каждым из участников процесса прохождения. Под исполнением документа подразумевается выполнение действия, связанного с документом, каждым из участников в рамках его должностных полномочий;
* генерация отчетов. Служат аналогом конторских журналов учета документов. Используя различные отчеты, можно посмотреть, например, общее время, потраченное сотрудниками на работу над конкретным документом, скорость прохождения документов по подразделениям и т.д. Отчеты — отличный материал для принятия управленческих решений;
* администрирование. Поддержка работы самой системы, настройки ее параметров и т. д.

СЭД относятся к системам локализованной или распределенной, двухуровневой или трехуровневой архитектуры.

Основными компонентами СЭД с трехуровневой архитектурой являются:

* сервер СУБД — сервер, обеспечивающий управление хранилищем атрибутов документов и (в большинстве случаев) хранилищем документов;
* сервер приложений СЭД — сервер, обеспечивающий реализацию бизнес-логики СЭД;
* клиент сервера приложений — приложение, функционирующее на компьютере пользователя и управляющее взаимодействием между пользова­телем и сервером приложений, а также («толстый клиент») частично реализующее бизнес-логику системы в части обработки конкретного доку­мента, интеграции с офисными пакетами, вывода на внешние устройства и т.п.

В общем случае в состав СЭД могут также входить следующие типовые компоненты ИТС: ФС ЛВС, РС ЛВС, устройства коммутации, устройства маршрутизации, каналы передачи данных.

**2. Угрозы информации, характерные для систем**

**электронного документооборота**

Особенности СЭД как объекта защиты:

* обязательность выполнения требований законодательства в области использования электронного документооборота и электронной цифровой подписи (ЭЦП): необходимость надежного сохранения архива документов; необходимость защиты целостности, подтверждения причастности к созданию и приему документов;
* разные способы организации хранилища документов;
* интеграция с офисными пакетами с необходимостью импорта/экспорта временных файлов;
* возможность прохождения части маршрута прохождения документа вне пределов организации (в системах распределенной архитектуры).

Основными информационными ресурсами, подлежащими защите в СЭД (информационными активами), являются: электронные документы; наборы данных атрибутов электронных документов (учетные карточки); наборы данных о маршрутах прохождения электронных документов.

Электронные документы могут быть представлены в виде следующих информационных объектов:

* неструктурированные записи (файлы) при сохранении в хранилище электронных документов (ФС, сервер СУБД);
* неструктурированные файлы в процессе сохранения и обработки на РС клиента;
* неструктурированные сообщения при передаче по каналам сети передачи данных (в системах распределенной архитектуры);
* информационные объекты в оперативной памяти компьютеров (сервер приложений, сервер СУБД, ФС, РС — в процессе обработки).

В штатном режиме функционирования СЭД к данным информационным объектам возможен разделяемый доступ с целью просмотра/ модификации.

Наборы данных атрибутов электронных документов могут быть представлены в виде следующих информационных объектов:

* структурированные записи при сохранении в хранилище атрибутов электронных документов (ФС, сервер СУБД);
* структурированные сообщения при передаче по каналам сети передачи данных (в системах распределенной архитектуры);
* информационные объекты в оперативной памяти компьютеров (сервер приложений, сервер СУБД, ФС, РС — в процессе обработки).

В штатном режиме функционирования СЭД к данным информацион­ным объектам возможен разделяемый доступ.

Наборы данных о маршрутах прохождения электронных документов могут быть представлены в виде следующих информационных объектов:

* структурированные записи при сохранении в хранилище (ФС, сервер СУБД);
* информационные объекты в оперативной памяти компьютеров (сервер приложений, сервер СУБД, ФС, РС - в процессе обработки).

В штатном режиме функционирования СЭД к данным информационным объектам невозможен разделяемый доступ с целью просмотра/ модификации.

Наиболее значимыми (с точки зрения наносимого информационным активам ущерба) типами угроз информации в СЭД являются угрозы с целью нарушения:

* конфиденциальности информации, содержащейся в электронных документах и наборах атрибутов документов, путем несанкционированного ознакомления;
* целостности информации, содержащейся в электронных документах, наборах атрибутов документов, наборах данных о маршрутах прохождения электронных документов, путем несанкционированной модификации;
* целостности информации, содержащейся в электронных документах, наборах атрибутов документов, путем отказа от авторства или отказа от получения;
* доступности разделяемых ресурсов сервера приложений (реализующего бизнес-логику), сервера СУБД (реализующего функции управления хранилищем электронных документов и хранилищем атрибутов электронных документов), ФС, на которых функционируют серверы приложений и серверы СУБД и размещаются хранилища данных.

**3. Модель потенциального нарушителя**

**в системе электронного документооборота**

В качестве потенциального нарушителя в СЭД должны рассматриваться:

1) любой сотрудник организации, использующей СЭД, внешний по отношению к автору/ редактору/ получателю конкретного электронного документа (в системах локализованной или распределенной архитектуры);

2) любой внешний по отношению к организации, использующей СЭД, пользователь ИТС (в системах распределенной архитектуры).

Сотрудник организации, использующей СЭД, внешний по отношению к автору/ редактору/ получателю конкретного электронного документа:

* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к обрабатываемым и сохраняемым в СЭД с использованием разделяемых ресурсов (ФС, сервер приложений, сервер СУБД) электронным документам (с целью их просмотра, модификации, уда­ления или создания нового документа);
* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к обрабатываемым и сохраняемым в СЭД с использованием разделяемых ресурсов (ФС, сервер приложений, сервер СУБД) наборам данных атрибутов электронных документов (с целью их про­смотра, модификации, удаления или создания нового набора атрибутов);
* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к обрабатываемым и сохраняемым в СЭД с использованием разделяемых ресурсов (ФС, сервер приложений, сервер СУБД) наборам данных о маршрутах электронных документов (с целью их модификации, удаления или создания нового набора данных);
* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к временно хранимым на РС клиента СЭД электронным документам (с целью их перехвата);
* с использованием штатных и нештатных средств может влиять на работоспособность разделяемых ресурсов СЭД (ФС, серверы СУБД, серверы приложений) и активного сетевого оборудования;
* обладает всеми возможностями пользователя СЭД по созданию, редактированию, передаче, просмотру документов, наборов данных атрибутов документов и наборов данных маршрутов документов.

Внешний по отношению к организации, использующей СЭД, пользователь ИТС (в системах распределенной архитектуры) с учетом того, что не вся инфраструктура сети передачи данных находится под контролем организации:

* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к передаваемым по каналам передачи данных электронным документам (с целью их перехвата, модификации, удаления или создания нового документа);
* может осуществить несанкционированный доступ (с использованием штатных и нештатных средств) к передаваемым по каналам передачи данных наборам данных атрибутов электронных документов (с целью их просмотра, модификации, удаления или создания нового набора атрибутов);
* с использованием штатных и нештатных средств может влиять на работоспособность разделяемых ресурсов СЭД, взаимодействующих с сетью передачи данных (серверы СУБД, серверы приложений, ФС, на которых функционируют серверы приложений и серверы СУБД и размещаются хранилища данных), активного сетевого оборудования и оборудования сети передачи данных.

Таким образом, потенциальный нарушитель имеет возможность реализации всех типов угроз (конфиденциальности, целостности и доступности) с использованием штатных средств СЭД, штатных и нештатных средств ОС, используемых ФС, штатных и нештатных средств серверов СУБД, штатных и нештатных средств серверов приложений, штатных и нештатных средств управления активным сетевым оборудованием и оборудованием сети передачи данных.

**4. Особенности построения систем защиты информации**

**в системе электронного документооборота**

Особенности построения систем защиты: обязательность администра­тивного управления доступом; обязательность ролевого управления доступом; обязательность выполнения требований законодательства в области использования электронного документооборота и ЭЦП; необходимость обеспечения надежного сохранения архива документов; необходимость защиты информации как внутри системы, так и на уровне ОС; необходимостью защиты временных файлов; необходимость защиты информации при обмене в случае прохождения части маршрута вне пределов организации.

В составе СЗИ СЭД можно выделить:

* подсистему управления;
* подсистему разграничения доступа;
* подсистему криптографической защиты;
* подсистему обнаружения атак и антивирусной защиты.

**5. Заключение**

Системы электронного документооборота (СЭД) — системы, предназначенные для автоматизации процессов создания, учета и обработки документов в электронном виде (электронных документов).

В качестве потенциального нарушителя в СЭД должны рассматриваться:

1) любой сотрудник организации, использующей СЭД, внешний по отношению к автору/ редактору/ получателю конкретного электронного документа (в системах локализованной или распределенной архитектуры);

2) любой внешний по отношению к организации, использующей СЭД, пользователь ИТС (в системах распределенной архитектуры).

В составе СЗИ СЭД можно выделить:

* подсистему управления;
* подсистему разграничения доступа;
* подсистему криптографической защиты;
* подсистему обнаружения атак и антивирусной защиты.

## 6. Вопросы для контроля знаний

1. Что такое СЭД?
2. Перечислите основные функции компонентов СЭД.
3. Какие типовые компоненты могут входить в состав СЭД?
4. Перечислите структуры СЭД, а также их компоненты.
5. Что такое «карточка»?
6. Кто может быть потенциальным нарушителем в СЭД?
7. Назовите особенности построения систем защиты.
8. Перечислите состав средств защиты информации в СЭД.

**Рекомундуемый список литературы:**

[1] Тимошенко, А.А. Защита информации в специализированных информационно-телекоммуникационных системах / А.А.Тимошенко. Киев, 2010.

[2] Шаньгин, В.Ф. Информационная безопасность компьютерных си­стем и сетей: учеб. пособие / В.Ф.Шаньгин. М., 2011.

Преподаватель В.А. Сабило

Приложение К

**ПЛАН-КОНСПЕКТ лабораторного занятия**

**Дисциплина:** Защита компьютерной информации

**Тема занятия:** Защита баз данных средствами СУБД MS Access.

**Цели занятия:** изучитьнавыки защиты ПО и базы данных средствами СУБД MS Access.

**Задачи:** сформировать знания учащихся о защите баз данных средствами СУБД MS Access.

**Вид занятия:** лабораторное занятие.

**Предварительная подготовка:** обучающимся рассказывается теоретическая часть занятия, выдаются задания для проведения лабораторной работы, вспомогательная литература.

**Этапы занятия:**

1. Организационный момент (приветствие, проверка присутствующих);
2. Представление темы и цели занятия;
3. Изложение материала о СУБД MS Access, способах защиты ПО и баз данных средствами MS Access;
4. Краткая демонстрация материала, связанного с темой;
5. Ответы на вопросы учащихся (при их наличии);
6. Выдача заданий;
7. Выполнение заданий обучающимися;
8. Подведение итогов работы: сдача отчетов, демонстрация выполненного задания учащимися, ответы на появившиеся вопросы.

**Конспект:**

**Способы защиты баз данных**

MS Access обеспечивает два традиционных способа защиты базы данных.

Простейший способ защиты — это установка пароля, требуемого при открытии базы данных. Тогда при каждом открытии базы данных будет появляться диалоговое окно, в котором требуется ввести пароль. Этот способ достаточно надежен, т. к. MS Access шифрует пароль, и к нему нет прямого доступа при чтении файла базы данных. После открытия базы данных все ее объекты становятся полностью доступными в течение сеанса работы с базой. Можно считать эту меру защиты достаточной для баз данных, которые сов­местно используются небольшой группой пользователей или установлены на автономном компьютере.

Гораздо более надежным и гибким способом организации защиты яв­ляется защита на уровне пользователей. Такой способ защиты позволяет ограничить возможность получения или изменения той или иной информации в базе данных для конкретного пользователя.

По умолчанию в базе определены две группы пользователей: Admins и Users. Для каждой группы задаются разрешения на доступ к объектам базы данных (права доступа). Члены группы Admins, как правило, имеют разрешения на доступ ко всем объектам базы данных. Поскольку группа Users объединяет всех пользователей, имеет смысл ей присваивать некоторый минимальный набор прав. Можно создавать собственные учетные записи групп, предоставляя этим группам соответствующие разрешения и добавляя в группы пользователей, исходя из функциональной специфики предметной области. Один и тот же пользователь может являться членом различных групп.

Как группам, так и пользователям предоставляются разрешения на доступ, определяющие допустимые для них действия по отношению к каждому объекту базы данных. Набор возможных прав, очевидно, определяется спецификой объекта. При запуске MS Access от пользователей требуется идентифицировать себя и ввести пароль.

Система безопасности БД должна обеспечивать физическую целостность БД и защиту от несанкционированного вторжения с целью чтения содержимого и изменения данных.

Защита БД производится на двух уровнях:

* на уровне пароля;
* на уровне пользователя (защита учетных записей пользователей и идентифицированных объектов).

Для защиты БД Ассеss использует файл рабочих групп systеm.mdw (рабочая группа — это группа пользователей, которые совместно используют ресурсы сети), к которому БД на рабочих станциях подключаются по умолчанию. Файл рабочих групп содержит учётные записи пользователей и групп, а также пароли пользователей. Учётным записям могут быть предоставлены права на доступ к БД и её объектам, при этом сами разрешения на доступ хранятся в БД.

Для обеспечения защиты БД Ассеss необходимо создать рабочую группу, используя файл - администратор рабочих групп wrkgаdm.еxе. При создании уникальной рабочей группы задается имя пользователя, название организации и код рабочей группы.

Файл рабочей группы MS Ассеss содержит следующие встроенные учётные записи:

Аdmins — стандартная учётная запись пользователя. Данные записи являются одинаковыми для всех экземпляров Мs Ассеss;

Аdmin — учётная запись группы администратора - является уникальной в каждом файле рабочей группы;

Usеrs — содержит учётные записи пользователей.

Для создания файла рабочих групп необходимо выйти из Ассеss и в папке systеm или systеm32 в каталоге windоws найти файл рабочей группы и создать новую рабочую группу (может быть до 20 цифровых или буквенных обозначений).

Группа Аdmins может содержать произвольное число пользователей, но владелец объекта всегда один (владельцем объекта может быть учётная запись, которая создавала объект или которой были переданы права на его использование).

Так как чтение записи Аdmin возможно для всех рабочих групп и данные учётные записи являются одинаковыми, то пользователя АDМIN необходимо удалить из группы администраторов, для чего следует создать новую учётную запись администратора и задать пароль на его учётные записи и на учетные записи владельца. Зашифровать и дешифровать базу данных могут только её владелец и члены группы Admins. Для шифрования Jet использует алгоритм RSA (назван по первым буквам фамилий его изобретателей: Rivest, Shamir, Adelman) с ключом на основе идентификатора рабочей группы.

У шифрования базы данных имеется два негативных побочных эффекта. Во-первых, снижается её быстродействие - по оценкам Microsoft, процентов на 10-15. Во-вторых, зашифрованную базу данных нельзя сжимать такими программами, как PKZip, LHA, Stacker и DriveSpace. Точнее, сжимать можно, только в этом нет смысла — её размер уменьшится незначительно.

**Разграничение прав доступа пользователей**

Разрешения к доступу называются явными, если они принадлежат или присвоены учётной записи пользователя. Разрешения будут неявными, если они присвоены учётной записи группы, при этом пользователь, включённый в группу получает все её разрешения.

|  |  |  |
| --- | --- | --- |
| Монопольный доступ | Монопольное открытие БД | БД |
| Чтение макета | Просмотр объектов в режиме конструктора | Таблицы, запросы, формы, отчеты, макросы и модули |
| Изменение макетов | Просмотр и изменение макетов, удаление | Таблицы, запросы, формы, отчеты, макросы и модули |
| Разрешения администратора | Установка пароля в БД, репликация БД | Предоставление прав доступа другим пользователям |
| Чтение данных | Просмотр данных | Таблицы и запросы |
| Обновление данных | Просмотр и измене­ние данных без удаления и вставки | Таблицы и запросы |
| Вставка данных | Просмотр и вставка данных без удаления и изменения | Таблицы и запросы |
| Удаление данных | Просмотр и удаление данных без измене­ния и вставки | Таблицы и макросы |

Полномочия пользователя определяются по минимальным разрешениям доступа. Изменить разрешения для пользователей могут члены группы Аdmins, владелец объекта и пользователь, получивший на этот объект разрешения администратора.

При подключении к БД пользователи получают права групп, которым они принадлежат.

**Задание к работе:**

1. Создать новую базу данных MS Access;
2. Зашифровать базу данных паролем.
3. Расшифровать базу данных.

**Вспомогательная литература:**

[1] Гурвиц, Г. Microsoft Access 2010. Разработка приложений на реальном примере / Г. Гурвиц. - М.: БХВ-Петербург, 2017. - 496 c.

[2] Бекаревич, Юрий Самоучитель Access 2010 / Юрий Бекаревич , Нина Пушкина. - М.: БХВ-Петербург, 2014. - 432 c.

**Рекомундуемый список литературы:**

[1] Защита баз данных на примере MS ACCESS // Пятифан [Электронный ресурс]. – Режим доступа: http://5fan.ru/wievjob.php?id=35031. – Дата доступа: 28.05.2020.

[2] Организация защиты данных в СУБД MS Access // Интуит [Электронный ресурс]. – Режим доступа: https://www.intuit.ru/studies/courses/3632/8

74/lecture/14303?page=8. – Дата доступа: 28.05.2020.

Преподаватель В.А. Сабило

Приложение Л

**Инструкция для лабораторного занятия**

Министерство образования Республики Беларусь

Учреждение образования

Филиал Белорусского государственного университета

информатики и радиоэлектроники

«Минский радиотехнический колледж»

Дисциплина «Защита компьютерной информации»

**Инструкция**

по выполнению лабораторной работы

«Защита баз данных средствами СУБД MS Access»

Минск

2020

Составитель: Сабило В.А.\_\_

Обсуждена и одобрена на заседании методической комиссии.

Протокол от \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_

**Лабораторная работа № 1**

**Тема работы: «Защита баз данных средствами СУБД MS Access»**

**1. Цель работы:** изучить метод защиты баз данных средствами СУБД MS Access.

**2. Задачи:**

1. обучающая:
2. сформировать знания учащихся о защите баз данных средствами СУБД MS Access;
3. воспитательная:
4. способствовать воспитанию усидчивости, организованности, дисциплинированности;
5. развивающая:
6. способствовать развитию умений учащихся обобщать полученные знания, проводить анализ, синтез, сравнения, делать необходимые выводы;
7. способствовать развитию коммуникативных навыков, логического мышления, самостоятельности, ответственности.

**3. Задание для самостоятельной работы:**

3.1. Создать новую базу данных MS Access.

3.2 Зашифровать базу данных паролем.

3.3. Расшифровать базу данных.

**4. Оснащение работы:** персональный компьютер, приложение MS Access.

**5. Основные теоретические сведения:**

Система безопасности БД должна обеспечивать физическую целостность БД и защиту от несанкционированного вторжения с целью чтения содержимого и изменения данных.

Защита БД производится на двух уровнях:

* на уровне пароля;
* на уровне пользователя (защита учетных записей пользователей и идентифицированных объектов).

Для защиты БД Ассеss использует файл рабочих групп systеm.mdw (рабочая группа - это группа пользователей, которые совместно используют ресурсы сети), к которому БД на рабочих станциях подключаются по умолчанию. Файл рабочих групп содержит учётные записи пользователей и групп, а также пароли пользователей. Учётным записям могут быть предоставлены права на доступ к БД и её объектам, при этом сами разрешения на доступ хранятся в БД.

Для обеспечения защиты БД Ассеss необходимо создать рабочую группу, используя файл - администратор рабочих групп wrkgаdm.еxе. При создании уникальной рабочей группы задается имя пользователя, название организации и код рабочей группы.

Файл рабочей группы MS Ассеss содержит следующие встроенные учётные записи:

1. Аdmins - стандартная учётная запись пользователя. Данные записи являются одинаковыми для всех экземпляров Мs Ассеss;

2. Аdmin - учётная запись группы администратора - является уникальной в каждом файле рабочей группы;

3. Usеrs - содержит учётные записи пользователей.

Для создания файла рабочих групп необходимо выйти из Ассеss и в папке systеm или systеm32 в каталоге windоws найти файл рабочей группы и создать новую рабочую группу (может быть до 20 цифровых или буквенных обозначений).

Группа Аdmins может содержать произвольное число пользователей, но владелец объекта всегда один (владельцем объекта может быть учётная запись, которая создавала объект или которой были переданы права на его использование).

Так как чтение записи Аdmin возможно для всех рабочих групп и данные учётные записи являются одинаковыми, то пользователя АDМIN необходимо удалить из группы администраторов, для чего следует создать новую учётную запись администратора и задать пароль на его учётные записи и на учетные записи владельца.

Зашифровать и дешифровать базу данных могут только её владелец и члены группы Admins. Для шифрования Jet использует алгоритм RSA (назван по первым буквам фамилий его изобретателей: Rivest, Shamir, Adelman) с ключом на основе идентификатора рабочей группы.

У шифрования базы данных имеется два негативных побочных эффекта. Во-первых, снижается её быстродействие - по оценкам Microsoft, процентов на 10-15. Во-вторых, зашифрованную базу данных нельзя сжимать такими программами, как PKZip, LHA, Stacker и DriveSpace. Точнее, сжимать можно, только в этом нет смысла - её размер уменьшится незначительно.

Разграничение прав доступа пользователей

Разрешения к доступу называются явными, если они принадлежат или присвоены учётной записи пользователя. Разрешения будут неявными, если они присвоены учётной записи группы, при этом пользователь, включённый в группу получает все её разрешения.

Таблица 1. Типы разрешений на доступ к БД

|  |  |  |
| --- | --- | --- |
| Разрешения | Разрешённые действия | Объекты БД |
| Открытие и  запуск | Открытие БД, формы или отчёта | БД, формы, отчёты, макросы |
| Монопольный доступ | Монопольное открытие БД | БД |
| Чтение макета | Просмотр объектов в режиме конструктора | Таблицы, запросы, формы, отчёты, макросы и модули |
| Изменение  макетов | Просмотр и изменение макетов, удаление | Таблицы, запросы, формы, отчёты, макросы и модули |
| Разрешения  администратора | Установка пароля в БД, репликация БД | Предоставление прав доступа другим пользователям |
| Чтение данных | Просмотр данных | Таблицы и запросы |
| Обновление данных | Просмотр и изменение данных без удаления и вставки | Таблицы и запросы |
| Вставка данных | Просмотр и вставка данных без удаления и изменения | Таблицы, запросы |
| Удаление данных | Просмотр и удаление данных без из изменения и вставки | Таблицы, макросы |

Полномочия пользователя определяются по минимальным разрешениям доступа. Изменить разрешения для пользователей могут члены группы Аdmins, владелец объекта и пользователь, получивший на этот объект разрешения администратора.

При подключении к БД пользователи получают права групп, которым они принадлежат.

**6. Порядок выполнения работы:**

6.1. Открыть СУБД MS Access и создать новую базу данных MS Access.

6.2. Создать в БД таблицу с данными (на свою тематику).

6.3. Сохранить созданную БД и закрыть эту БД.

6.4. Вновь открыть БД но уже в монопольном режиме.

* на вкладке «Файл» нажать кнопку «Открыть»;
* в диалоговом окне «Открыть» найти файл, который нужно открыть, и выделите его;
* щелкнуть стрелку рядом с кнопкой «Открыть» и выбрать команду «Монопольно».

6.5. На вкладке «Файл» нажать кнопку «Сведения» и выбрать пункт «Зашифровать паролем».

6.6. В открытом диалоговом окне «Задание пароля базы данных» ввести пароль в поле «Пароль», а затем повторите его в поле «Проверить».

6.7. Закрыть БД.

6.8. Открыть защищенную паролем БД в монопольном режиме. В появившемся окне «Необходимо ввести пароль» ввести пароль.

6.9. Удалить установленный пароль (выполнить «Файл»-«Сведения»-«Расшифровать базу данных»).

6.10. В появившемся окне «Удаление пароля баз данных» ввести пароль.

6.11. Оформить отчет по рекомендуемой форме.

**7. Форма отчета о работе:**

*Лабораторная работа № \_\_\_*

*Номер учебной группы \_\_\_\_\_\_\_\_*

*Фамилия, инициалы обучающегося \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*Дата выполнения работы \_\_\_\_\_\_\_\_\_\_\_\_*

*Тема работы: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*Цель работы: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*Задание: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*Оснащение работы: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*Результаты выполнения работы: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

Отчет по лабораторной работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в отпечатанном виде на листах формата А4.

Отчет должен содержать:

1. Название и цель лабораторной работы;
2. Скриншоты о проделанной работе;
3. Заключения и выводы.

**8. Контрольные вопросы и задания:**

1. Перечислите способы защиты информации в БД Access.
2. Какие существуют группы и пользователи БД Access?
3. Дайте определение понятию «Владелец объекта».
4. Перечислите типы разрешений на доступ к базе данных.
5. Перечислите объекты БД.
6. Расскажите алгоритм защиты БД Access.

**Рекомундуемый список литературы:**

[1] Гурвиц, Г. Microsoft Access 2010. Разработка приложений на реальном примере / Г. Гурвиц. - М.: БХВ-Петербург, 2017. - 496 c.

[2] Бекаревич, Юрий Самоучитель Access 2010 / Юрий Бекаревич , Нина Пушкина. - М.: БХВ-Петербург, 2014. - 432 c.

Приложение М

**Презентации лекционных занятий**

**Ведомость документов**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | | | | | Наименование | | | | | Дополнительные сведения | | |
|  | | | | | Текстовые документы | | | | |  | | |
|  | | | | |  | | | | |  | | |
| БГУИР КР 1-08 01 01-07 19 ПЗ | | | | | Пояснительная записка | | | | | 89 с. | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | | Электронные документы | | | | |  | | |
|  | | | | |  | | | | |  | | |
| БГУИР КР 1-08 01 01-07 19 Э | | | | | Мультимедиапрезентации для прове- | | | | | CD-R 1 шт. | | |
|  | | | | | дения лекционных занятий | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  | | | | |  | | | | |  | | |
|  |  |  |  |  | | БГУИР КР 1-08 01 01-07 19 Д1 | | | | | | |
|  |  |  |  |  | |
|  |  |  |  |  | |
| Изм. | Л. | № докум. | Подп. | Дата | | Методическая разработка раздела «Особенности построения систем защиты информации в информационных системах различного типа» по дисциплине «Защита компьютерной информации» уровня среднего специального образования  Ведомость курсовой  работы |  | | | | Лист | Листов |
| Разраб. | | Сабило В.А. |  | 11.05.20 | |  |  |  | | 89 | 89 |
| Пров. | | Парафиянович Т.А. |  | 11.05.20 | | Кафедра ИРТ  гр. 844691 | | | | | |
|  | |  |  |  | |
|  | |  |  |  | |
|  | |  |  |  | |