АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

УТВЕРЖДАЮ

ДИРЕКТОР АНО ПО «БИТ»

_____ В.В. СЕРГЕЕВ

«31» августа 20 20 ГОДА

М.П.

ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП. 01Основы информационной безопасности

2020г.

Программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее — ФГОС) по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного приказом Министерства образования и науки Российской Федерации 9 декабря 2016 года № 1548 и примерной основной образовательной программы СПО, разработанной ФУМО 2017 г.

Организация-разработчик: АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

Разработчик: _____Зыкова Ирина Анатольевна, преподаватель

Рассмотрена
на заседании цикловой методической комиссии №1, протокол № 1
от «31» августа 2020 г.
председатель ЦМК №1

_____О.О.Васильева

СОДЕРЖАНИЕ *СТР.*

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Область применения программы

Программа учебной дисциплины «Основы информационной безопасности» далее «Основы ИБ» является частью основной образовательной программы 4-поколения в соответствии с ФГОС СПО по специальности:

10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Основы ИБ» входит в вариативную часть общего гуманитарного и социально-экономического цикла дисциплин.

1.3. Цель и планируемые результаты освоения дисциплины:

– Учебная дисциплина «Основы ИБ» необходима для освоения студентами основных понятий информационной безопасности применяемых терминов;

– получение знаний по основным правовым понятиям, законодательным актам и другим нормативным документам в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации;

– получение знаний по классификации систем и средств, обеспечивающих информационную безопасность;

– освоение направлений, методов и способов достижения безопасности в информационных системах и каналах.

– передачи на всех этапах жизненных циклов источников информации ознакомление с методами управления информационными ресурсами, обеспечивающими сохранность и защиту информации в современных компьютерных комплексах, системах и сетях,

– доведение уровня знаний у студентов до способности воспринимать и обучаться по таким дисциплинам как, технические средства защиты информации.

В результате освоения дисциплины обучающийся должен **знать**:

– видs и источникb угроз информационной безопасности и мерs по их предотвращению;

– основы правовых, организационных и инженерно-технических направлений защиты информации;

– законодательство РФ в области защиты государственной тайны, открытой и конфиденциальной информации;

– основные руководящие документы, регламентирующие информационную безопасность на объектах защиты;

– жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи и т.д.;

– виды, средства и способы защиты информации, состав систем защиты информации;

В результате освоения учебной дисциплины обучающийся должен ***уметь***:

– оценить состояние информационной безопасности на объекте защиты и правильно определить зоны безопасности;

– правильно оформлять документы при подборе и увольнении кадров работающих с конфиденциальной информацией;

– выбирать рациональные меры по обеспечению информационной безопасности.

Изучение дисциплины «Основы информационной безопасности» обеспечивает овладение следующими компетенциями:

Общие компетентности (ОК):

- ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
- ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.
- ОК 6. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

Профессиональными компетенциями (ПК):

- ПК 1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
- П.К. 2 Способен изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации
- ПК- 3 способен применять комплексный подход к обеспечению безопасности в различных сферах деятельности
- ПК- 4. Контролировать работу компьютерных, периферийных устройств и телекоммуникационных систем, обеспечивать их безопасную и правильную эксплуатацию.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	*Объем часов*
Максимальная учебная нагрузка (всего)	80
Обязательная аудиторная учебная нагрузка (всего)	*60*
в том числе:	
лекционные занятия	*34*
практические занятия	
контрольные работы	
Самостоятельная работа обучающегося (всего)	*20*
внеаудиторная самостоятельная работа	*6*
Итоговая аттестация в форме экзамена	

2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

Наименование разделов и тем	**Содержание учебного материала и формы организации деятельности обучающихся**	**Объем Часов**	**Уровень Освоения**	**Осваиваемые элементы компетенций**
1	*2*	*3*	*4*	*5*
Введение	Введение в дисциплину. Основные этапы становления информационной безопасности в России. Самостоятельная работа Входной контроль	*2* *4*	*1* 5	ОК 2.4
Раздел 1 Системы защиты информации, ее концептуальные модели Тема 1. Сущность и понятие информационной безопасности, характеристика её составляющих.	Сущность защиты информации (ЗИ) и системы (СЗИ), понятие и определение информационной безопасности, характеристика её составляющих. Термины, применяемые в информационной безопасности. Входной контроль. **Самостоятельная работа.** Подготовка к входному контролю. **Практические занятия** – входной контроль методом тестирования на ПК.	*20* 6	2 2 3	ОК 2.3.4 ОКП5
Тема 3. Современная концепция информационной безопасности	Концептуальная модель информационной безопасности. Доктрина информационной безопасности РФ. Задачи по развитию ИБ в различных информационных	4	2	ОК 1.3.2 ПК 3

	сферах РФ. **Практические занятия** – семинар по темам Доктрины ИБ РФ с примерами из современной жизни. **Самостоятельная работа** – домашняя подготовка к семинару по темам Доктрины ИБ РФ.		3	ОК5.6
Тема 4. Понятие и сущность защиты информации.	Защита информации, как основная составляющая информационной безопасности. Организационно-технические методы осуществления защиты информации по различным каналам утечки информации.	2	3	ОК 2.3.5 ПК2
Тема 5. Цели и концептуальные основы защиты информации. Системы защиты информации.	Цели и концептуальные основы защиты кадровых, материально-технических и информационных ресурсов. Системы защиты информации.	4	1	ОК 2.5
Тема 6. Носители защищаемой информации, классификация по видам и группам	Классификация носителей: Механическая запись информации, бумажные носители, магнитные носители, электромагнитные носители (физ. поля). Демонстрация видов носителей, принципы магнитной записи. **Практические занятия**. Пример записи информации в аудитории, с последующим стиранием и её поэтапная	4	2 3 3	ОК 1.4. ПК3 ОК 2.3 ОКП5

	классификация по видам и группам. Исследование принципов магнитной записи. Дестабилизирующие воздействие на магнитные носители информации.			
Раздел 2 ***Федеральное регулирование*** ***вопросов информационной безопасности*** Тема 2.1 Классификация информации по видам тайны и степеням конфиденциальности.	Положения ФЗ «О государственной тайне», ФЗ «О коммерческой тайне» о принципах отнесения информации к секретам. Роль межведомственной комиссии по защите гос. тайны. **Практические занятия**. Классификация информации по видам тайны и степеням конфиденциальности. Опрос с примерами по рис. Л13 стр. 90	***22*** 2	2 3	ПК1.3 ОП 2.3.5 ОК2.6 ПК2 ОКП5
Тема 2.2 Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.	Цели и источники дестабилизирующего воздействия на защищаемую информацию (по Л1 – рис. 4,5 угрозы). Классификация угроз. (по объекту, по ущербу и т.п.). Методы (способы) дестабилизирующих воздействий на защищаемую информацию	4	3	ОК 2.3 ПК 1.4
Тема 2.3 Виды уязвимости информации и формы её	Воздействие угроз на конфиденциальность и	4	2	ПК 1.3 ОК 24

проявления.	целостность информации. Воздействие угроз на доступность к информации			
Тема 2.4 Технические каналы утечки и методы несанкционированного доступа к защищаемой информации. Презентация по теме.	Определение и классификация каналов утечки информации. Угрозы утраты, утечки, модификации информации	4	1	ПК1.2 ОК 2.3.4
Тема 2.5 Методологические подходы к защите информации и принципы её организации.	Основные методы и способы защиты информации. Энергетические (пассивные и активные) методы скрытия, информационное скрытие, дезинформация, как метод скрытия	4	1	ОК 2.3.5 ПК 2.3
Тема 2. 6 Объекты защиты, виды защиты	Виды физической охраны объектов защиты. Внутренние войска, ведомственная, вневедомственная, частные охранные предприятия. Службы безопасности на предприятиях, их структура. Задачи отделов информационной безопасности в СБ.	4	2	ОК 2.3.5 ПК 1.3
Раздел 3 **Ресурсное обеспечение защиты информации.** Тема 3.1 Системы защиты информации	Гос. система защиты информации, понятия о комплексных СЗИ. Вопросы лицензирования	***10*** 8	2	ОК 2.3 ПК 1.2.5

	деятельности по технической защите информации. История развития федеральной службы технического и экспортного контроля (ФСТЭК).			
Темы 3.2 Кадровое и ресурсное обеспечение защиты информации	Кадровое и ресурсное обеспечение защиты информации. Основные этапы подбора кадров и приёма на работу связанную с гос. секретами. Оформление допуска, понятие форм допуска (категорирование кадров) **Практические занятия.** Технология подбора кадров и увольнения Самостоятельная работа	4	2 3	ОК 3.1 ПК 1.2.5 ОКП5
Экзамен		*3*		

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т.п.);

2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Реализация программы дисциплины требует наличия учебного кабинета и компьютерного класса.

Технические средства обучения

Оборудование учебного кабинета:

1. посадочные места по количеству обучающихся;
2. рабочее место преподавателя;
3. доска;
4. проектор

Оборудование компьютерного класса и рабочих мест:

1. посадочные места по количеству обучающихся;
2. компьютер с лицензионным программным обеспечением;
3. Мультимедийное оборудование.

Основные источники:

1. В.И. Ярочкин «Информационная безопасность». Москва. 2014г
2. Т.Л.Партыка Информационная безопасность Москва «Форум-ИНФРА». 2013г
3. С.Н. Сёмкин, Э.В. Беляков «Основы организационного обеспечения информационной безопасности объектов информатизации». Учебное пособие. Москва «Гелиос АРВ». 2013г
4. А.Н. Соболев В.М. Кириллов «Физические основы технических средств обеспечения информационной безопасности». Москва «Гелиос АРВ». 2014г
5. Е.А. Степанов, И.К. Корнев «Информационная безопасность и защита информации», М.-ИНФРА-М, 2013г
6. В.А. Кудрявцев, Е.А. Степанов «Безопасность предпринимательской деятельности». М.:ГУУ, 2012

Законодательные источники

1. Федеральный закон РФ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» от 21 .09. 2013// журнал официальной информации: Кадастр, 2013. N 35 с.3-41
2. Федеральный закон «О лицензировании отдельных видов деятельности», N 128-ФЗ, от 08.08.2001 (в ред. ФЗ от13.03.2002 N 28-ФЗ, от 21.03.2002 N 31-ФЗ, от 09.12.2012 N 164-Фз, от27.02.2013 N 29-ФЗ)
3. Положение о государственном лицензировании деятельности в области защиты информации. Утверждено Решением Гостехкомиссии России и ФАПСИ от 27.04.2014 г. № 10.
4. Федеральный закон РФ «О КОММЕРЧЕСКОЙ ТАЙНЕ» N 98 ФЗ от 29.06.2012
5. Федеральный закон “об информации, информационных технологиях и о защите информации” 2006 г.
7. Доктрина информационной безопасности РФ. Стр. 341 в учебнике В.И. Ярочкин «Информационная безопасность». Москва. Принята в сентябре 2000 года.

Дополнительные источники:

8. Государственный стандарт Российской Федерации ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
9. Информационная безопасность и защита информации. Сборник терминов и определений. Гостехкомиссия России, 2011 г.
10. А.В. Солдатенков, А.В. Волокитин, А.П. Маношкин и др. «Информационная безопасность государственных организаций и коммерческих фирм», М.: Фиорд - ИНФА,

11. Основные положения сертификации технических средств электросвязи взаимоувязанной сети связи России (утв. Минсвязи РФ от 26 октября 2014 г.).

12. Презентации по предмету ОИБ составленные преподавателями и студентами 3-4 курсов специальности ИБАС.

Интернет-ресурсы:

1.http://fcior.edu.ru.

2. http://metodist.lbz.ru/authors/informatika.

3. http://in-sites.ru/html.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Передавать информацию устно и письменно с соблюдением требований к защите информации;	Оценка и анализ высказываний обучающихся при проведении беседы. Оценка и анализ высказываний обучающихся при индивидуальном и групповом опросе в устной форме. Оценка выполнения письменных и устных упражнений. Оценка содержания реферативных сообщений.
Анализировать выбираемые методы и средства защиты информации с точки зрения их нормативности, уместности и целесообразности; находить и устранять ошибки и недочёты в своих действиях и действиях студентов при проведении работ по обеспечению информационной безопасности;	Самооценка и взаимооценка высказываний обучающихся при проведении беседы, при индивидуальном и групповом опросе. Самооценка и взаимооценка выполнения письменных и устных упражнений.
Осуществлять профессиональное общение с соблюдением норм и правил обеспечивающих защиту информации в автоматизированных системах; Осуществлять разграничения по видам тайн. Соблюдением норм и правил обеспечивающих защиту информации в автоматизированных системах;	Оценка и анализ высказываний обучающихся при проведении беседы. Оценка и анализ высказываний обучающихся при индивидуальном и групповом опросе в устной форме. Оценка и взаимооценка обучающимися друг друга при анализе видеозаписей. Оценка и анализ диалогов, составленных обучающимися. Анализ высказываний, аргументов обучающихся при проведении дискуссии.

Пользоваться нормативно-правовыми актами;	Оценка умения пользоваться при выполнении письменных и устных упражнений.
Оформлять документацию по подготовке и внедрению систем защиты информации;	Оценка умения оформлять техническую документацию.
По результатам практической деятельности в лаборатории ТСЗИ осуществлять выбор технических средств защиты из предлагаемой номенклатуры СТС.	Оценка индивидуального и группового опроса в устной форме.