СОГЛАСОВАНО
Начальник отдела защиты информации
Министерства цифрового развития
Смоленской области
_____ А.Н. Калугин
«31» 08 2023 г.

УТВЕРЖДАЮ
Заместитель директора по
учебной работе
_____ И.В. Иванешко
«31» 08 2023 г.

Контрольно-оценочные средства для промежуточной аттестации УП. 03 Учебная практика, ПП. 03 Производственная практика по профессиональному модулю ПМ. 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи 11.02.15 Инфокоммуникационные сети и системы связи

Комплексный дифференцированный зачет является промежуточной формой контроля, подводит итог освоения УП.03, ПП.03 проверяет сформированность следующих профессиональных компетенций:

Код	Наименование профессиональных компетенций
ПК 3.1	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.
ПК 3.2	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.
ПК 3.3	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования

А также общих компетенций:

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

Промежуточный контроль по учебной и производственной практикам осуществляется в виде комплексного дифференцированного зачета (учебная и производственная практика в совокупности).

Комплексный дифференцированный зачет по УП.03 и ПП.03 проводится на основе тестирования по учебной практике, а также предоставленных документов: отчета по производственной практике в соответствии с требованиями оформления, дневника по практике, положительной характеристики работодателя и заполненного аттестационного листа.

Шкала перевода баллов в оценки:

Оценка результатов КДЗ	Количество баллов		
	УП.03	ПП.03 (аттестационный лист, дневник, положительное заключение работодателя)	ПП03 (отчет по практике)
«5» (отлично)	5 4	12 12	1 1
«4» (хорошо)	4 3	12 12	1 1
«3» (удовлетворительно)	3	12	1
«2» (неудовлетворительно)	2 5 4 3	Менее 12 Менее 12 Менее 12 Менее 12	0 0 0 0

В результате освоения УП.03 и ПП.03 студент должен:

Обязательная часть

иметь практический опыт:

ПО1 - анализировать сетевую инфраструктуру;

ПО2 - выявлять угрозы и уязвимости в сетевой инфраструктуре;

ПО3 - разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи;

ПО4 - осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи;

ПО5 - использовать специализированное программное обеспечения и оборудование для защиты инфокоммуникационных сетей и систем связи;

уметь:

У1 - классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;

У2 - проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;

У3 - определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;

У4 - осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;

У5 - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;

У6 - выполнять тестирование систем с целью определения уровня защищенности;

У7 - определять оптимальные способы обеспечения информационной безопасности;

У8 - проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;

У9 - проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;

У10 - разрабатывать политику безопасности сетевых элементов и логических сетей;

У11 - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;

У12 - производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;

У13 - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

У14 - защищать базы данных при помощи специализированных программных продуктов;

У15 - защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами;

знать:

З1 - принципы построения информационно-коммуникационных сетей;

З2 - международные стандарты информационной безопасности для проводных и беспроводных сетей;

З3 - нормативно - правовые и законодательные акты в области информационной безопасности;

З4 - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления и закрытия;

З5 - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;

З6 - способы и методы обнаружения средств съёма информации в радиоканале;

З7 - классификацию угроз сетевой безопасности;

З8 - характерные особенности сетевых атак;

З9 - возможные способы несанкционированного доступа к системам связи;

З10 - правила проведения возможных проверок согласно нормативных документов ФСТЭК;

З11 - этапы определения конфиденциальности документов объекта защиты;

З12 - назначение, классификацию и принципы работы специализированного оборудования;

З13 - методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP. WPA и WPA 2;

З14 - методы и средства защиты информации в телекоммуникациях от вредоносных программ;

З15 - технологии применения программных продуктов;

З16 - возможные способы, места установки и настройки программных продуктов;

З17 - методы и способы защиты информации, передаваемой по кабельным направляющим системам;

З18 - конфигурации защищаемых сетей;

З19 - алгоритмы работы тестовых программ;

З20 - средства защиты различных операционных систем и среды передачи информации;

З21 - способы и методы шифрования (кодирование и декодирование) информации.

Вариативная часть

уметь:

У16 - проводить мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

У17 - администрировать наложенные программно-аппаратных средства защиты информации от НСД;

У18 - применять программно-аппаратные комплексы глубокого анализа трафика;

У19 - производить выбор необходимых средств криптографической защиты информации;

У20 - применять программные средства, реализующие основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа;

У21 - вырабатывать рекомендации для принятия решения о модернизации системы защиты информации;

У22 - осуществлять мероприятия по защите персональных данных;

Знать:

З22 - состав работ по комплексной защите информации значимых объектов критической информационной инфраструктуры;

З23 - концепцию инженерно-технической защиты информации;

З24 - методы оценки угрозы инженерно-технического добывания информации;

З25 - основные принципы организации и методы реализации технической защиты информации;

З26 - методы аппаратурной оценки энергетических параметров побочных излучений от технических средств и систем передачи, хранения и обработки информации;

З27 - методы инженерного расчета размеров контролируемой зоны;

З28 - основные требования к системам криптографической защиты;

З29 - основные принципы организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСТЭК, ФСБ России;

З30 - этапы проведения аудита информационной безопасности информационных систем и объектов информатизации.

Тест содержит 40 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока (первый блок 60 вопросов, второй блок 60 вопросов) заданий по 20 вопросов.

Время тестирования – 90 минут (по 1,5 минуты на каждый вопрос тестовых позиций и по 2 минуты на краткие ответы теоретических вопросов). Время на подготовку и проверку тестирования – 20 минут.

Образцы аттестационных листов по практикам (приложение 1, приложение 4), требования к оформлению технического отчета (приложение 2), дневника практики, характеристики работодателя (приложение 3), ведомости (приложение 5) приводятся в приложениях.

Результаты определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», вносятся в итоговую ведомость комплексного дифференцированного зачета и объявляются в тот же день.

Шкала оценивания образовательных результатов тестирования:

Критерии	Кол-во баллов по тестированию
получают студенты, справившиеся с работой 100-90%;	5 баллов
получают студенты, справившиеся с работой 89-76%	4 балла
получают студенты, справившиеся с работой 60-75%	3 балла
менее 60% правильных ответов	От 0 до 2 баллов

Блок заданий закрытого типа Формируемые ПК 3.1 – ПК 3.3, ОК 01 – ОК 09		
1.	Что из перечисленного является основными угрозами доступности информации?	1.Непреднамеренные ошибки пользователей. 2.Злонамеренное изменение данных 3.Хакерская атака. 4.Отказ программного и аппаратного обеспечения. 5.Разрушение или повреждение помещений. 6.Перехват данных.
2.	Какая политика безопасности реализуется при помощи матрицы доступа?	1. Мандатное управление доступом. 2. Ролевая политика управления доступом. 3. Избирательное управление доступом
3.	Какая политика безопасности реализуется при помощи назначения грифов доступа различным объектам?	1. Мандатное управление доступом. 2. Ролевая политика управления доступом. 3. Избирательное управление доступом
4.	Какие бывают модели доступа?	1. Дискреционная (DAC), 2. Комплексная (CAC) 3. Мандатная (MAC). 4. Ролевая (RBAC). 5. Все ответы верны.
5.	Для чего применяется разграничение прав доступа в сети?	1. Для защиты данных от утечки. 2. Для защиты от нецелевого использования данных. 3. Для контроля целостности данных. 4. Для анализа событий и разбора инцидентов.
6.	Что такое замкнутая программная среда (ЗПС)?	1. ЗПС является средством повышения безопасности ОС путем контроля доступности файлов. 2. ЗПС является средством повышения безопасности ОС путем контроля целостности файлов. 3. ЗПС является средством, обеспечивающим защиту от исполнения стороннего ПО и внедрённого вредоносного кода.
7.	В чем состоит отличие системы по обнаружению вторжений (СОВ или в	1.Это по сути один класс систем с одинаковыми функциональными возможностями.

	зарубежной терминологии IDS) и системы по предотвращению вторжений (СПВ или IPS)?	2.Это по сути два отдельных класса систем с разными функциональными возможностями. 3.Это по сути два отдельных класса систем с одинаковыми функциональными возможностями.
8.	Что из перечисленного относится к основным функциям систем IDS?	Выявление вторжений и сетевых атак. Запись всех событий. Прогнозирование возможных уязвимостей в системе Информирование служб ИБ об инциденте в реальном времени.
9.	Что из перечисленного относится к основным функциям систем IDS?	1.Распознавание источника атаки: инсайд или взлом. 2.Поиск уязвимостей. 3.Информирование служб ИБ об инциденте по запросу. 4.Прогнозирование атак.
10.	По каким методам работают технологии IPS?	1.Сигнатурный анализ. 2.Эвристический анализ. 3.Математический анализ. 4.Поведенческий анализ.
11.	Что из перечисленного относится к ключевым функциям IPS?	1.Прекращение доступа к хостам, обрыв сессии сотрудника, нелегитимно обращающегося к данным. 2.Изменение конфигурации устройств в сети компании для предотвращения атаки. 3.Удаление или фильтрация инфицированных файлов перед отправкой пользователям на уровне сетевых пакетов. 4.Все ответы верны.
12.	Что такое сигнатура?	1.Это шаблон для выявления источника вторжений и сетевых атак. 2.Это шаблон, по которому определяется атака через сравнение с возможным инцидентом. 3.Это шаблон для выявления источника атаки: инсайд или взлом.
13.	Каких типов бывают системы IPS/IDS?	1. NIDS. 2. APIDS. 3. PIDS. 4. HIDS. 5.Гибридные.
14.	Для каких целей служат сетевые (NIDS) IPS/IDS системы?	1.Для проверки специализированных прикладных протоколов. 2.Для проверки сетевого трафика с коммутатора. В основе лежит протокол СОВ (PIDS) - мониторит трафик по HTTP и HTTPS-протоколами. 3.Анализируют журналы приложений, состояние хостов, системные вызовы. 4.Объединяют функции нескольких видов систем обнаружения вторжений.
15.	Для каких целей служат IPS/IDS системы, основанные на прикладных протоколах СОВ (APIDS)?	1.Для проверки специализированных прикладных протоколов. 2.Для проверки сетевого трафика с коммутатора. В основе лежит протокол СОВ (PIDS) - мониторит трафик по HTTP и HTTPS-протоколами. 3.Анализируют журналы приложений, состояние хостов, системные вызовы. 4.Объединяют функции нескольких видов систем обнаружения вторжений.
16.	Для каких целей служат Host-Based (HIDS) IPS/IDS системы?	1.Для проверки специализированных прикладных протоколов. 2.Для проверки сетевого трафика с коммутатора. В основе лежит протокол СОВ (PIDS) - мониторит трафик по HTTP и HTTPS-протоколами. 3.Анализируют журналы приложений, состояние хостов,

		системные вызовы. 4.Объединяют функции нескольких видов систем обнаружения вторжений.
17.	От каких злоумышленных действий защищает система IDS / IPS?	1.От проблем с доступом к сайту и сервисам компании. 2. От проникновения во внутреннюю сеть компании. 3. От целенаправленных атак с целью кражи данных или средств. 4. Все ответы верны.
18.	Какие типы из перечисленных атак распознает система IDS / IPS?	1.Атаки типа «отказ в обслуживании» (DoS). 2.Использование уязвимостей и вредоносного ПО. 3.Повышение привилегий пользователя. 4. Все ответы верны.
19.	Какие типы из перечисленных атак распознает система IDS / IPS?	1.Атаки методом грубой силы. 2.Использование вредоносного ПО. 3.Неавторизованный доступ. 4. Все ответы верны.
20.	Что понимается под атакой на информационную систему?	1.Любое действие, нарушающее безопасность информационной системы. 2.Действие или последовательность связанных между собой действий, использующих уязвимости информационной системы, и приводящих к нарушению политики безопасности. 3.Использование ошибок в программном обеспечении. 4.Исключительно несанкционированный доступ в систему.
21.	Каким образом функционируют системы обнаружения атак на уровне узла?	1.Осуществляют мониторинг активности одного узла в сети. 2.Осуществляют мониторинг активности всех сегментов сети. 3.Осуществляют консолидацию и хранение журналов событий от различных источников. 4.Предоставляют инструменты для анализа событий и разбора инцидентов.
22.	Каким образом функционируют системы обнаружения атак на уровне сети?	1.Осуществляют мониторинг сетевого сегмента. 2.Осуществляют мониторинг активности одного узла в сети. 3.Осуществляют консолидацию и хранение журналов событий от различных источников. 4.Предоставляют инструменты для анализа событий и разбора инцидентов.
23.	Что из перечисленного способна выявлять SIEM система?	1.Вирусные эпидемии или отдельные вирусные заражения, не удаленные вирусы, бэкдоры и трояны. 2.Попытки несанкционированного доступа к конфиденциальной информации. 3.Фрод и мошенничество. 4.Все ответы верны.
24.	Что из перечисленного выполняет SIEM система?	1.Технология SIEM отслеживает инциденты безопасности в корпоративной сети. 2.Технология SIEM анализирует журналы приложений, состояние хостов, системные вызовы. 3.Технология SIEM осуществляет консолидацию и хранение журналов событий от различных источников. 4.Технология SIEM генерирует оповещения и выполняет аудит всех действий, связанных с инцидентом.
25.	Что из перечисленного является основными задачами SIEM системы?	1.Сбор, обработка и анализ событий безопасности. 2.Сканирование на наличие уязвимостей как с учетной записью администратора, так и без нее. 3.Регистрация инцидентов в режиме реального времени. 4. Поиск остаточной информации по ключевым словам на носителях данных вне зависимости от файловой

		структуры. 5.Оперативная оценка защищенности информационных, телекоммуникационных и других критически важных ресурсов.
26.	Что из перечисленного является основными задачами SIEM системы?	1.Анализ и управление рисками безопасности. 2.Инвентаризация программных и аппаратных средств локальной системы, включая историю подключений к беспроводным сетям, данные системных, коммуникационных и периферийных устройств. 3.Проведение расследований инцидентов. 4.Принятие эффективных решений по защите информации. 5.Формирование отчетных документов.
27.	Что такое защищенный канал связи?	1. Гарантированное исключение любых атак в реальном времени на канал связи. 2.Гарантированное исключение доступа к передаваемой информации третьих лиц. 3. Гарантированная сохранность только важной информации.
28.	Для каких целей предназначен ViPNet Coordinator?	1. Для защиты сегментов IP-сетей. 2. Для создания VPN-сети на основе технологии ViPNet. 3.Для защиты трафика, передаваемого по открытым каналам связи. 4.Для координации работы узлов защищенной сети.
29.	В чем состоит преимущество технологии VPN на основе симметричной криптографии?	1.Позволяют быстро построить VPN-сеть любой масштабности, не обращая внимания на адресную структуру. 2.Позволяют размещать VPN-модули на компьютерах внутри локальных сетей, защищенных NAT-устройствами. 3.Позволяют размещать VPN-модули на компьютерах за пределами локальных сетей. 4.Позволяют размещать VPN-модули на VPN-шлюзах на границе локальных сетей.
30.	Какие функции из перечисленных выполняет ViPNet Coordinator?	1.Выполняет функции персонального и межсетевого экрана. 2.Создание и модификация структуры сети ViPNet. 3.Создает туннели для организации защищенных соединений с открытыми узлами.
31.	Какие функции из перечисленных выполняет ViPNet Coordinator?	1.Позволяет разделить доступ защищенных узлов в Интернет и к ресурсам локальной сети. 2.Разграничение уровней полномочий пользователей сети ViPNet. 3.Позволяет исключить любые атаки в реальном времени на компьютеры локальной сети.
32.	Какие функции из перечисленных выполняет ViPNet Coordinator?	1.Создание и модификация структуры сети ViPNet. 2.Издание и управление сертификатами пользователей. 3. Осуществляет трансляцию адресов (NAT) для проходящего через координатор открытого трафика.
33.	Из каких компонентов состоит ViPNet Administrator?	1.Удостоверяющий центр. 2.Центр управления сетью. 3.Удостоверяющий и ключевой центр. 4.Ключевой центр.
34.	Какие функции из перечисленных выполняет Центр управления сетью?	1.Создание и модификация структуры сети ViPNet. 2.Издание и управление сертификатами пользователей. 3.Отправка ключевой и справочной информации, обновлений ПО ViPNet на сетевые узлы.
35.	Какие функции из перечисленных выполняет Центр управления сетью?	1.Выполняет функции персонального и межсетевого экрана. 2.Разграничение уровней полномочий пользователей сети ViPNet.

		3.Позволяет исключить любые атаки в реальном времени на компьютеры локальной сети.
36.	Какие функции из перечисленных выполняет Удостоверяющий и ключевой центр?	1.Формирование и управление ключевой структурой сети. 2.Издание и управление сертификатами пользователей. 3.Отправка ключевой и справочной информации, обновлений ПО ViPNet на сетевые узлы.
37.	Какие записи должны вестись при аудите?	1.Вход/выход пользователей. 2.Неудачные попытки входа. 3.Все системные события 4.Зависит от уровня аудита.
38.	Что из перечисленного относится к локальному аудиту информационной безопасности корпоративной системы?	1.Аудит стойкости паролей для операционных систем. 2. Поиск остаточной информации по ключевым словам на носителях данных вне зависимости от файловой структуры. 3.Безагентное сканирование на наличие уязвимостей как с учетной записью администратора, так и без нее. 4.Очистка информации на носителях данных путем многократного затирания файлов по стандартам ГОСТ, BSI, FIPS, DoD. 5.Контроль появления новых сетевых узлов и сервисов, идентификация ОС и приложений, трассировка маршрутов передачи данных, построение топологии сети организации.
39.	Что из перечисленного относится к сетевому аудиту информационной безопасности корпоративной системы?	1.Обнаружение, сканирование и проведение активных и пассивных атак методом подбора паролей в беспроводных сетях с WEP, WPA и WPA-2 шифрованием. 2.Инвентаризация программных и аппаратных средств локальной системы, включая историю подключений к беспроводным сетям, коммуникационных и периферийных устройств. 3.Сравнение отчетов, которое позволяет отслеживать изменения конфигурации системы. 4.Аудит настроек комплекса средств защиты ОС специального назначения «Astra Linux Special Edition» по требованиям безопасности.
40.	Что из перечисленного относится к сетевому аудиту информационной безопасности корпоративной системы?	1.Инвентаризация программных и аппаратных средств локальной системы, включая историю подключений к беспроводным сетям, данные системных, коммуникационных и периферийных устройств. 2.Проверка стойкости паролей всех сетевых сервисов, требующих авторизации. 3.Поиск подходящих эксплойтов на основе собранной информации об узле. 4.Перехват и анализ трафика, фильтрация содержимого передаваемых данных, а также реализация атак типа MITM. 5.Подсчет контрольных сумм заданных папок и файлов по алгоритмам, включая алгоритмы высокой стойкости к атакам ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012.
41.	Для чего используют сканер ВС?	1. С помощью Сканера-ВС можно выявлять источники вторжений и сетевых атак. 2.С помощью Сканера-ВС можно проводить тестирование на проникновение. 3.С помощью Сканера-ВС можно проводить анализ конфигурации. 4. С помощью Сканера-ВС можно выявлять источники атаки: инсайд или взлом.
42.	Для чего используют сканер ВС?	1.С помощью Сканера-ВС можно проводить сканирование уязвимостей. 2. С помощью Сканера-ВС можно выявлять источники вторжений и сетевые атаки.

		3.С помощью Сканера-ВС можно организовать непрерывный контроль защищенности. 4. Все ответы верны.
43.	Что из перечисленного относится к сетевому аудиту информационной безопасности корпоративной системы?	1.Контроль появления новых сетевых узлов и сервисов, идентификация ОС и приложений, трассировка маршрутов передачи данных, построение топологии сети организации. 2.Очистка информации на носителях данных путем многократного затирания файлов по стандартам ГОСТ, BSI, FIPS, DoD. 3.Безагентное сканирование на наличие уязвимостей как с учетной записью администратора, так и без нее. 4. Поиск остаточной информации по ключевым словам на носителях данных вне зависимости от файловой структуры. 5.Формирование отчета с техническими рекомендациями по устранению обнаруженных брешей в защите.
44.	Что из перечисленного относится к локальному аудиту информационной безопасности корпоративной системы?	1.Инвентаризация программных и аппаратных средств локальной системы, включая параметры установленных операционных систем, программное обеспечение, информацию о пользователях системы. 2.Проверка стойкости паролей всех сетевых сервисов, требующих авторизации. 3.Поиск подходящих эксплойтов на основе собранной информации об узле. 4.Инвентаризация программных и аппаратных средств локальной системы, включая историю подключений к беспроводным сетям, данные системных, коммуникационных и периферийных устройств.
45.	Что из перечисленного относится к локальному аудиту информационной безопасности корпоративной системы?	1.Перехват и анализ трафика, фильтрация содержимого передаваемых данных, а также реализация атак типа MITM. 2.Сравнение отчетов, которое позволяет отслеживать изменения конфигурации системы. 3.Формирование отчета с техническими рекомендациями по устранению обнаруженных брешей в защите. 5.Подсчет контрольных сумм заданных папок и файлов по алгоритмам, включая алгоритмы высокой стойкости к атакам ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012.
46.	Что такое анализ защищенности ИТ-инфраструктуры?	1.Анализ защищенности – это контролируемое техническое воздействие, направленное на выявление минимального количества уязвимостей в исследуемой ИТ-инфраструктуре. 2.Анализ защищенности – это контролируемое техническое воздействие, направленное на выявление максимального количества уязвимостей и недостатков в исследуемой ИТ-инфраструктуре или информационной системе. 3.Анализ защищенности – это организационное воздействие, направленное на выявление потерь от угрозы информационной безопасности в исследуемой ИТ-инфраструктуре или информационной системе.
47	Что происходит в информационной системе при использовании IDS?	1.Возрастает возможность определения преамбулы атаки. 2.Возрастает возможность фильтрования трафика. 3.Возрастает возможность определения оптимального маршрута для каждого вида трафика. 4.Возрастает возможность раскрытия осуществленной атаки.
48.	Каким образом могут быть реализованы IDS?	1.Только программно. 2.Только аппаратно. 3.Только совместно с межсетевым экраном.

		4.Как программно, так и аппаратно.
49.	Какие правила использования ресурсов сети применяют для разграничения доступа на уровне файловой системы?	1.Правила фильтрации межсетевого экрана. 2.Списки управления доступом 3.БД политик безопасности. 4.Списки разрешенных ресурсов.
50.	Какие задачи решаются при проведении анализа защищенности?	1.Выполнение требований регуляторов. 2.Получение представления о текущем уровне защищенности системы. 3.Оценка защищенности ИТ-инфраструктуры и эффективности используемых механизмов защиты. 4.Получение подробной картины уязвимостей и недостатков исследуемой системы. 5.Все, перечисленное в остальных пунктах.
51.	Каковы преимущества использования системы унифицированного управления угрозами?	1.Увеличивается пропускная способность сети. 2.Уменьшается сложность управления. 3.Увеличивается безопасность сетевого периметра. 4.Уменьшается количество попыток несанкционированного доступа.
52.	Когда рекомендуется проводить работы по анализу защищенности?	1.При первичной установке информационной системы. 2.При публикации новой версии используемой ИС. 3.При внесении существенных изменений в систему или инфраструктуру. 4.Все, перечисленное в остальных пунктах.
53.	Для каких целей применяют систему контроля доступа?	1.Предотвратить проникновение на частную территорию посторонних лиц. 2.Организовать учет рабочего времени, фиксацию времени въезда и выезда транспортных средств. 3.Защитить материальные ценности, включая производственное и офисное оборудование, от повреждений и кражи. 4.Все ответы верны.
54.	Что анализируется в IDS при определении злоупотреблений?	1.Анализируются события на соответствие некоторым образцам, называемым «сигнатурами атак». 2.Анализируются события для обнаружения неожиданного поведения. 3.Анализируются подписи в сертификатах открытого ключа. 4.Анализируется частота возникновения некоторого события.
55.	Что анализируется в IDS при определении аномалий?	1.Анализируется частота возникновения некоторого события. 2.Анализируются различные статистические и эвристические метрики. 3.Анализируются события на соответствие некоторым образцам, называемым «сигнатурами атак». 4.Анализируется исключительно интенсивность трафика.
56.	Какие шаги следует предпринять при обнаружении подозрительного трафика?	1.Идентифицировать систему. 2.Записывать в журнал сведения о дополнительном трафике между источником и пунктом назначения. 3.Заблокировать удаленную систему. 4.Записывать в журнал весь трафик, исходящий из источника.
57.	Что могут определить атаки сканирования?	1.Топологию целевой сети. 2.Типы сетевого трафика, пропускаемые межсетевым экраном. 3.Номера версий для всего обнаруженного ПО. 4.Все ответы верны.
58.	Каковы общие свойства систем анализа уязвимостей и систем	1.И те, и другие следят за конкретными симптомами проникновения и другими нарушениями политики

	обнаружения вторжений?	безопасности. 2.И те, и другие могут фильтровать трафик. 3.И те, и другие могут шифровать трафик. 4.И те, и другие могут аутентифицировать пользователей.
59.	Каковы преимущества использования IDS?	1.Возможность иметь реакцию на атаку. 2.Возможность блокирования атаки. 3.Выполнение документирования существующих угроз для сети и систем. 4.Нет необходимости в межсетевых экранах.
60.	Для каких целей устанавливается IDS?	1.Обнаружение атак 2.Предотвращение атак 3.Обнаружение нарушений политики безопасности. 4.Повышение надежности системы.

Блок заданий открытого типа
Формируемые ПК 3.1 - ПК 3.3, ОК 01 – ОК 09

1.С какой целью проводится анализ защищенности объекта защиты информации?

2.Какие средства чаще всего используются для проведения анализа защищенности ИТ-инфраструктуры?

3.Где устанавливается система обнаружения вторжений уровня сети и что она контролирует?

4.Где устанавливается система обнаружения вторжений уровня узла и что она анализирует?

5.Какие системы автоматизируют процесс управления учетными записями, например, управляют процессом по созданию, изменению и блокированию учетных записей?

6. Какое программное решение, выступает в роли посредника между пользователем браузера и веб-сервером, подменяя сертификаты пользователя и сервера?

7. Какое программное решение выступает в роли посредника между пользователем браузера и веб-сервером, и защищает внутренние веб-ресурсы организации?

8.Какая модель доступа базируется на явно заданных для каждого пользователя правах доступа к объектам информации, и представляются в виде матрицы, в которой указываются полномочия относительно каждого объекта информации?

9.В какой модели доступа всем субъектам (сотрудникам) и объектам (файлам, папкам и т.д.) назначаются метки (мандаты), соответствующие разным уровням конфиденциальности?

10.Какой компонент управления доступом требует от пользователей подтверждения своей личности с использованием как минимум двух или более различных факторов проверки, прежде чем получить доступ к какому-либо ресурсу?

11.Какой открытый стандарт системы аутентификации предоставляет пользователю возможность создания единой учётной записи для аутентификации на множестве не связанных друг с другом интернет-ресурсов, используя услуги третьих лиц?

12.Какой пароль, действителен только для одного сеанса аутентификации, действие этого пароля также может быть ограничено определённым промежутком времени?

13. Как называется технология однократного ввода учетных данных для доступа к нескольким системам/приложениям?

14.Какой класс решений обеспечивает контроль и защиту мобильных устройств, используемых организацией и её сотрудниками?

15. Как называется набор распределённых служб и компонентов, используемых для поддержки криптозадач, на основе закрытого и открытого ключей?

16.Как называется процесс оценки подозрительных действий в защищаемой сети, который реализуется либо анализом журналов регистрации операционной системы и приложений, либо сетевого трафика?

17.Сколько выделяют классов систем обнаружения атак по принципу реализации и какие?

18.В каком подходе к обнаружению атак системы обнаружения атак осуществляют поиск шаблонов известных атак в сетевом трафике или высокоуровневых данных?

19. В каком подходе к обнаружению атак системы обнаружения атак имеют профиль нормальной активности системы и детектируют отклонения от него?

20.Какие системы обнаружения атак, состоят из множества IDS, которые расположены в различных участках сети, связаны между собой и с центральным управляющим сервером?

21.Какие программные или аппаратные системы сетевой и компьютерной безопасности обнаруживают вторжения и автоматически защищают от них?

22.Как называют два основных этапа работ по анализу защищенности, проводимых по отношению к периметру корпоративной сети?

23.Какие программы способны перехватывать и анализировать сетевой трафик и полезны в тех случаях, когда нужно извлечь из потока данных какие-либо сведения (например, пароли), или провести диагностику сети?

24.Какие программы используются для удаленного управления рабочими станциями или другими компьютерными устройствами?

25. Как называется процесс проверки инфраструктуры компании на наличие проблем и слабых мест, которые могут быть связаны с ошибками конфигурации или используемым ПО?

26. Какие программные и аппаратные средства используются для обнаружения неавторизованного входа в систему, а также неправомерных и несанкционированных попыток по управлению защищаемой сетью?

27. Как называется единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа?

28.Какая учетная запись имеет больше прав, чем стандартная учетная запись, объем прав таких записей зависит от должностных обязанностей и используемых технологий?

29.Как называется процесс сбора и анализа информации об ИС и реализованных организационно-технических мерах защиты для оценки уровня ее защищенности?

30.Какой сетевой протокол прикладного уровня служит для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия?

31.Какой криптографический сетевой протокол служит для безопасного управления сетевыми службами в незащищенной сети?

32.Какой криптографический протокол обеспечивает защищённую передачу данных между узлами в сети Интернет?

33.Какие средства безопасности предназначены для анализа защищенности информации в корпоративных сетях и могут выполнять проверку сетевых устройств, учетных записей ОС, установленных patch'ей системы безопасности ОС?

34.Какая система безопасности защищает от негативного воздействия внешних злоумышленников, а именно от DoS-атак, работы ботнетов, работы хостов, зараженных троянским ПО и сетевыми червями, спам-сетей?

35. К какому виду программно-технических средств обеспечения информационной безопасности относят системы обнаружения и предотвращения вторжений (IDS/IPS) и системы предотвращения утечек конфиденциальной информации (DLP-системы)?

36. К какому виду программно-технических способов и средств обеспечения информационной безопасности относят пароль; ключ доступа (физический или электронный); сертификат?

37. Какое СЗИ обеспечивает защиту от загрузки произвольного исполняемого файла или библиотеки, не обладающих корректной ЭЦП?

38. Какая система безопасности позволяет оптимизировать обработку и мониторинг действий учетных записей с повышенными привилегиями?

39. Какая технология используется для защиты информации в сети ViPNet?

40.Что такое носитель ключевой информации?

41. Какие существуют методы защиты каналов передачи данных?

42. Что содержит комплекс системных мер по обнаружению вредоносной активности в корпоративной сети?

43.В чем суть сигнатурного анализа трафика сети передачи данных, или сопоставления шаблонов/сигнатур?

44. Как работает эвристический анализатор трафика сети передачи данных?

45. Для чего служит контент-фильтр?

46. Что такое многоуровневая защита информации?

47. Для каких целей используются защищенные сети VPN?

48. Как реализуется защита данных в VPN-сети?

49. Какими способами можно построить VPN-канал?

50. Какая VPN защищает данные, передаваемые между узлами корпоративной сети, находящимися в одном сетевом сегменте, и также применяется для разделения одной физической сети на несколько логических?

51.Как называется свободная реализация технологии VPN для создания зашифрованных каналов типа точка-точка или сервер-клиент, позволяющая устанавливать соединения между компьютерами, находящимися за NAT-firewall?

52.Какой туннельный протокол типа точка-точка, позволяет компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети?

53.Какие виртуальные сети реализуются для обеспечения защищенного канала между корпоративной сетью и пользователем, подключенным к защищенной сети извне, например, с домашнего ПК?

54.Какие VPN реализуются провайдерами для предоставления доступа клиентам, подключающимся по одному физическому каналу связи?

55. Какими способами защищают базы данных?

56.Какое решение по защите от вирусов используют для защиты пользователей от угроз, приходящих извне (с веб-сайтов и зараженных файлов, скачиваемых через веб-браузер)?

57. Какие программные или программно-аппаратные средства защиты позволяют осуществлять запуск операционной системы исключительно с доверенных носителей информации (например, жестких дисков)?

58.Какие VPN сети называются доверительными сетями?

59. Какие программные или программно-аппаратные средства защиты обеспечивают охрану данных от возможной утечки внутри компании?

60. Для чего нужно контролировать и регулировать доступ пользователей внутренней сети к ресурсам общедоступной сети?

Составил преподаватель Грубник Е.М.

Заведующий практикой Драницина М.Д.

РАССМОТРЕНО
на заседании методической
комиссии дисциплин
средств подвижной связи
Председатель _____Е.Н. Кожекина
Протокол №__ _____20__ г.

СОГЛАСОВАНО
на заседании методической комиссии
общепрофессиональных и многоканальных
телекоммуникационных дисциплин
Председатель _____ Ващенкова Т.В.
Протокол №_____
«___» _____ 20___ г.

Приложение 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

СМОЛЕНСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ (ФИЛИАЛ) СПбГУТ
(СКТ(ф)СПбГУТ)

АТТЕСТАЦИОННЫЙ ЛИСТ ПО УЧЕБНОЙ ПРАКТИКЕ

_____
ФИО

Обучающийся(аяся) на ___ курсе в группе _____ по специальности СПО

11.02.15 Инфокоммуникационные сети и системы связи
код *наименование*

успешно прошел(ла) **учебную** практику по профессиональному модулю

ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи
наименование профессионального модуля

в объеме 36 часов с ___ _____ 202__ по ___ _____ 202__ в организации

Смоленский колледж телекоммуникаций (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»
наименование организации

г. Смоленск, ул. Коммунистическая, д.21
юридический адрес

Виды и качество выполнения работ

Виды работ, выполненных студентом во время практики	*Отметка о выполнении*
1. Реализация политик безопасности в системах и сетях на примере дискреционных и мандатных прав доступа (6 часов). 2. Проведение анализа защищенности объекта защиты информации (6 часов). 3. Проведение инструментальных проверок объекта защиты информации (6 часов). 4. Организация защиты каналов связи при подключении к защищенным ресурсам с использованием технологии ViPNet (6 часов). 5. Организация защищенного общения корпоративных пользователей (на примере ViPNet CSS Connect) (6 часов). 6. Управление системой обнаружения вторжений (на примере «Континент СОВ») (6 часов).	
Количество баллов по тестированию: _____	

Характеристика учебной и профессиональной деятельности студента во время учебной практики.
Аттестуемый(ая) продемонстрировал(а) / не продемонстрировал(а) владение общими и профессиональными компетенциями:

_____

Код	Наименование результата обучения
ПК 3.1	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.
ПК 3.2	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.
ПК 3.3	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

Дата _____.
Подпись(и) руководителя(ей) практики

Преподаватель _____
подпись *расшифровка подписи*
Преподаватель _____
подпись *расшифровка подписи*

Заведующий практикой М.Д. Драницина

Приложение 2

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

СМОЛЕНСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ (ФИЛИАЛ) СПбГУТ
(СКТ(ф)СПбГУТ)

ТЕХНИЧЕСКИЙ ОТЧЕТ

по производственной практике

студента _____
ФИО

ПМ. 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

по специальности 11.02.15 Инфокоммуникационные сети и системы связи

г.Смоленск
20___ г.

Т Р Е Б О В А Н И Я
ПО СОСТАВЛЕНИЮ ТЕХНИЧЕСКОГО ОТЧЕТА
ПО ПРАКТИКЕ

Технический отчет по производственной практике студенты пишут во время прохождения практики в соответствии с графиком учебного процесса.

Технический отчет должен быть выполнен на стандартных листах писчей бумаги (ф. А 4), в объеме 10-12 страниц.

Перечень вопросов технического отчета следующий:

- титульный лист
- программа практики
- введение
- 1.Общие сведения о функциях и структуре предприятия (схема структуры предприятия)
- 2.Описание производственного процесса участка, на котором проходит основной период производственной практики.
- 3.Индивидуальное задание по ПМ.
- 4.Организация и состояние охраны труда на предприятии.
- Список литературы.
- Приложение (фото, аудио-файлы при их наличии).

Технический отчет должен быть оформлен в соответствии с требованиями (СТО 1.1-2015) – требования к выполнению текстовых документов:

- Текст отчета должен быть выполнен на компьютере с одинаковым межстрочным интервалом (1,0).
- Отчет выполняется на листах с одной стороны, разборчиво, аккуратно, четко.
- Текст набирается нежирным шрифтом Times New Roman на стандартных листах 14 шрифтом с соответствующей рамкой, границы которой располагаются следующим образом:

- расстояние слева от границы листа до рамки – 20 мм.
- расстояние сверху, справа и снизу от границы листа до рамки 5 мм.

- Текст каждого листа записи должен иметь следующие поля:

- расстояние слева от текста до рамки 5мм, справа от текста до рамки 3мм.
- расстояние от заголовка, верхней и нижней строки текста до рамки 10 мм.
- абзацы в тексте начинаются отступом 15мм.

- В отчет обязательно должны входить структурные, функциональные схемы.
- Нумерация страниц обязательна.

5. Технический отчет должен быть проверен и подписан руководителем практики от предприятия и заверен печатью.

6. Технический отчет сдается заведующему практикой от колледжа для получения комплексного дифференциального зачета.

Заведующий практикой Драницина М.Д.

Утверждаю
Зам.директора по учебной работе

_____ Иванешко И.В.

ПРОГРАММА ПРАКТИКИ

Название МДК	Виды работ в соответствии с рабочими программами МДК	Количество часов
МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи	Вводный инструктаж по месту проведения практики. Изучение правил внутреннего трудового распорядка, правил охраны труда. Изучение деятельности организации в целом и избранного структурного подразделения. Ознакомление со структурой и работой основных подразделений организации.	6
	Изучение типовых документов, регламентирующих вопросы защиты информации (справочно-информационных, стандартов, ГОСТов, руководящих документов); возможности обеспечения единого нормативно-правового регулирования процессов защиты информации; возможности создания на предприятии (организации) условий для понимания существующих проблем по защите информации.	6
	Изучение требований, предъявляемых к обеспечению информационной безопасности на объекте информатизации, разработка политик безопасности в системах и сетях.	6
	Ознакомление с информационной системой безопасности предприятия (организации), используемыми техническими средствами и программными продуктами, составление краткой характеристики информационной системы.	6
	Изучение применяемых технологий и технических средств, используемых в целях обеспечения защиты информации на объекте.	6
	Участие в организации прав доступа к информации, изучение особенностей работы сотрудников по защите государственных интересов, особенностей работы организации по защите коммерческих интересов, наличия в организации перечня сведений, относящихся к коммерческой тайне, утвержденных приказом по организации.	6
	Участие в процедуре разграничения коммерческой информации по группам: деловая информация; техническая информация; информация о клиентах и конкурентах; изучение существующих в организации механизмов защиты конфиденциальной информации; участие в работе специальной структуры и подразделения по защите информации; изучение периодичности издания на предприятии приказов, распоряжений, инструкций по защите информации.	6
	Участие в реализации применения методов анализа факторов, влияющих на уровень защиты информации, применения технических и программных средств по защите информации.	6
	Участие в реализации криптографических методов защиты информации, защиты информации в сетях ЭВМ и персональных компьютерах.	6
	Обработка и систематизация критического и фактического материала, анализ полученной информации и практического опыта применения комплекса методов и средств защиты информации в инфокоммуникационных сетях.	6
	Выполнение индивидуального задания по производственной практике.	6
	Написание отчета по практике, оформление дневника практики и его визирование руководителем практики от организации. Получение отзыва руководителя практики. Комплексный дифференцированный зачет с УП.03, ПП.03.	6
	Всего	72

Индивидуальное задание (1-2 вопроса практического характера, составляются преподавателями данного ПМ):

1.

2

Примерные вопросы на производственную практику

1.Управление пользователями в JaCarta Management System.
2. Проверка работоспособности защитных модулей WEB ANTIFRAUD.
3. Функциональные возможности Group-IB Fraud Hunting Platform.
4. Архитектура системы аутентификации на базе JaCarta U2F.
5. Сценарии использования SafeNet Authentication Service.
6. Управление SafeNet eToken.
7. Сценарии использования Silverfort.
8. Функциональные возможности и работа с ESET Secure Authentication 3.0.
9. Функциональные возможности и блокировка сайтов SkyDNS.
10. Сценарии использования FortiIsolator.
11. Функциональные возможности и развертывание «Гарда БД 4».
12. Развертывание и настройка СЗИ ВИ Dallas Lock.
13. Управление учетными записями в СЗИ ВИ Dallas Lock.
14.Архитектура и функциональные возможности KES Cloud и KES Cloud Plus.
15. Архитектура и функциональные особенности Kaspersky Security для виртуальных сред.
16. Функциональные возможности и работа с vGate 4.1.
17. Сценарии использования СПО «Аккорд-KVM».
18. Функциональные возможности и сценарии использования McAfee Web Gateway.
19. Сценарии использования UserGate Log Analyzer.
20. Функциональные возможности и работа с Solar webProxy.
21. Применение Solar webProxy.
22. Функциональные возможности и сценарии SurfSecure.
23. Функциональные возможности и варианты подключения StormWall.
24. Функциональные возможности и сценарии работы услуги «Облачная защита от DDoS-атак» компании «МегаФон».
25. Функциональные возможности и сценарии использования AVSOFT ATHENA.
26. Технологии, используемые в Kaspersky Threat Management and Defense.
27.Архитектура и сценарии использования СЗИ НСД Dallas Lock Linux.
28. Функциональные возможности и использование программного модуля доверенной загрузки уровня UEFI BIOS ViPNet SafeBoot.
29. Функциональные возможности и практические примеры настройки «Континент» 3.9.
30. Функциональные возможности и сценарии использования СКЗИ «Квазар» для криптографической защиты каналов связи.
31. Функциональные возможности и работа с КриптоПро DSS.
32.Функциональные возможности и сценарии использования UserGate X10.
33. Функциональные возможности и работа с ИТ-активами в MaxPatrol VM.
34. Основные функциональные возможности и применение UserGate Management Center
35. Функциональные возможности и сценарии использования комплекса для защиты удалённых рабочих мест сотрудников САКУРА.
36. Функциональные возможности и сценарии использования InfoWatch Vision.
37. Основные возможности Dozor FC и работа с Dozor File Crawler.
38. Принцип работы и основные возможности IGA-системы Solar inRights.
39. Функциональные возможности и сценарии использования Ideco UTM 10.
40. Функциональные возможности универсального шлюза безопасности ИКС 7.2.

Председатель методической комиссии Кожекина Е.Н.

Приложение 3

ДНЕВНИК
производственной практики

_____

ФИО

Группа

Специальность 11.02.15 Инфокоммуникационные сети и системы связи

успешно прошел(ла) производственную практику по профессиональному модулю:
ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

в объеме 72 часа с «___» _____20___г. по «___» _____20___г.

В организации

_____

адрес организации

Дата	Краткое описание работ, выполненных студентом во время практики	Отметка руководителя практики от предприятия о выполненной работе (подпись)

Последний день практики	сдача КДЗ в колледже	

Отношение студента-практиканта к работе (организация собственной деятельности), оформляется руководителем практики от предприятия

Дата _____ _____ 202__ г.

Подпись руководителя практики от предприятия _____ _____
ФИО *подпись*

Приложение 4

АТТЕСТАЦИОННЫЙ ЛИСТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

ФИО

Обучающийся (аяся) на 3 курсе в группе ____ по специальности СПО

Специальность 11.02.15 Инфокоммуникационные сети и системы связи

успешно прошел(ла) производственную практику по профессиональному модулю

ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

в объеме 72 часов с «___» _____20___г. по «___» _____20___г.

в организации

юридический адрес

Виды работ, выполненных студентом во время практики:

Прошел вводный инструктаж по месту проведения практики. Изучил правила внутреннего трудового распорядка, правила охраны труда. Изучил деятельность организации в целом и избранного структурного подразделения. Ознакомился со структурой и работой основных подразделений организации.
Изучил типовые документы, регламентирующие вопросы защиты информации (справочно-информационные, стандарты, ГОСТы, руководящие документы); возможность обеспечения единого нормативно-правового регулирования процессов защиты информации; возможность создания на предприятии (организации) условий для понимания существующих проблем по защите информации.
Изучил требования, предъявляемые к обеспечению информационной безопасности на объекте информатизации, разрабатывал политики безопасности в системах и сетях.
Ознакомился с информационной системой безопасности предприятия (организации), используемыми техническими средствами и программными продуктами, составил краткую характеристику информационной системы.
Изучил применяемые технологии и технические средства, используемые в целях обеспечения защиты информации на объекте.
Участвовал в организации прав доступа к информации, изучил особенности работы сотрудников по защите государственных интересов, особенности работы организации по защите коммерческих интересов, наличие в организации перечня сведений, относящихся к коммерческой тайне, утвержденных приказом по организации.
Участвовал в процедуре разграничения коммерческой информации по группам: деловая информация; техническая информация; информация о клиентах и конкурентах; изучил существующие в организации механизмы защиты конфиденциальной информации; участие в работе специальной структуры и подразделения по защите информации; изучение периодичности издания на предприятии приказов, распоряжений, инструкций по защите информации.
Участвовал в применении методов анализа факторов, влияющих на уровень защиты информации, применении технических и программных средств по защите информации.
Участвовал в реализации криптографических методов защиты информации, защиты информации в сетях ЭВМ и персональных компьютерах.
Обрабатывал и систематизировал критический и фактический материал, анализировал полученную информацию и практический опыт применения комплекса методов и средств защиты информации в инфокоммуникационных сетях.
Выполнил индивидуальное задание по производственной практике.
Подготовил отчет по практике, оформил дневник практики. Сдал комплексный дифференцированный зачет с УП.03, ПП.03.
Характеристика учебной и профессиональной деятельности студента во время производственной практики Аттестуемый(ая) *продемонстрировал(а) / не продемонстрировал(а)* владение профессиональными и общими компетенциями

С целью овладения видом деятельности ВД 3 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» обучающимся были освоены общие и профессиональные компетенции:			
Наименование ОК	Баллы (0-1) 0 - не освоена, 1- освоена	Наименование ПК	Баллы (0-1) 0 - не освоена, 1- освоена
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.		3.1.Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.	
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.		3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.		3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования	
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.			
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.			
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.			
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.			
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.			
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.			
Общее количество баллов:_____ *Максимальное кол-во набранных баллов: 12* *Минимальное кол-во баллов: -0*			

Руководитель практики от предприятия:

_____	_____	_____
должность	*подпись*	*расшифровка*

Дата _____ _____ 20….. г.

МП

Приложение 5

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

СМОЛЕНСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ (ФИЛИАЛ) СПбГУТ
(СКТ(ф)СПбГУТ)

В Е Д О М О С Т Ь

20__/20__ учебный год

УП.03 Учебная практика
ПП.03 Производственная практика (по профилю специальности)
ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

Курс _____ группа _____

Специальность 11.02.15 Инфокоммуникационные сети и системы связи

Преподаватель _____
(фамилия, имя, отчество)

№№ пп	ФИО студента	Кол-во баллов по УП.03	Кол-во баллов по ПП.03	Кол-во баллов по отчету	Оценка результата КДЗ
……	……..				

Преподаватель _____ _____
(фамилия, имя, отчество)

Заведующий практикой _____ М.Д.Драницина

«___» _____ 20___ г.