Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

ПРИНЯТО

на заседании педагогического совета
Протокол № 2
«26» декабря 2023 г.

УТВЕРЖДАЮ
Директор СПб ГБПОУ «АУГСГиП»
А.М. Кривоносов
«26» декабря 2023 г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

по текущему контролю успеваемости
и промежуточной аттестации
по профессиональному модулю
ПМ.05 УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация
Техник по защите информации

Форма обучения
очная

Санкт-Петербург
2023 год

Комплект контрольно-оценочных средств по профессиональному модулю ПМ.05 Управление информационной безопасностью разработан на основе Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки России от 09.12.2016 № 1553.

СОГЛАСОВАНО
ООО «ДЖИ-ТИ ИНВЕСТ»
Генеральный директор
_____ П.С. Тюганов
«26» декабря 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

СОДЕРЖАНИЕ

1. ПАСПОРТ КОМПЛЕКТА ОЦЕНОЧНЫХ СРЕДСТВ

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности по участию в управлении информационной безопасностью и составляющих его профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ППССЗ в целом.

Комплект контрольно-оценочных средств позволяет оценивать:

1. Освоение профессиональных компетенций (ПК), соответствующих виду профессиональной деятельности, и общих компетенций (ОК):

Код	Наименование результата обучения
ПК 5.1	Применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК 5.2	Проводить контроль соблюдения персоналом требований режима защиты информации
ПК 5.3	Проводить экспертизу при расследовании компьютерных преступлений
ПК 5.4	Принимать участие в организации закупки оборудования
ПК 5.5	Принимать участие в управлении проектами
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 9.	Использовать информационные технологии в профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере

2. Освоение умений и усвоение знаний:

№	**Освоенные умения, усвоенные знания**

№	**Освоенные умения, усвоенные знания**
31	принципы формирования политики информационной безопасности в информационных системах,
32	основы организации и методологии проведения аудита ИБ,
33	основные методы управления инцидентами,
34	основные стандарты управления ИБ,
35	методики анализа рисков, программные средства анализа и управления рисками,
36	требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров,
37	требования режима защиты информации при приеме в организации посетителей,
38	организацию работы при осуществлении международного сотрудничества,
39	задачи, функции и структуру подразделений защиты информации,
310	принципы, методы и технологию управления подразделений защиты информации,
311	методы проверки персонала по защите информации,
312	процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией;
313	методы сбора; обработки и анализа информации;
314	положения федерального законодательства о контрактной системе в сфере закупок и иных сопутствующих нормативных правовых актов;
315	основные этапы проведения закупки, требований законодательства к организации и проведению процедур определения поставщика при применении различных способов закупки;
316	основные понятия «проект» и «проектный менеджмент»;
317	методы управления проектами;
318	цели проекта и требования, предъявляемые к проекту;
319	окружение и участников проекта;
320	жизненный цикл и структуру проекта;
321	способы определения длительности проекта;
322	правила разработки расписания проекта;
323	правила проведения анализа критического пути проекта;
324	методы оценки стоимости проекта;

№	**Освоенные умения, усвоенные знания**
З25	понятие и основные этапы оценки эффективности проекта;
З26	классификацию и методы оценки проектных рисков;
З27	виды коммуникаций их роль в рамках проекта
У1	разрабатывать частные политики информационной безопасности информационных систем,
У2	разрабатывать организационно-распорядительные документы системы менеджмента,
У3	проводить расследование инцидентов информационной безопасности организации;
У4	организовывать деятельность по обнаружению и реагированию на инциденты информационной безопасности в организациях, информационных системах,
У5	анализировать и оценивать информационные риски;
У6	разрабатывать модели угроз и нарушителей информационной безопасности информационных систем
У7	разрабатывать предложения по совершенствованию системы управления информационной безопасностью,
У8	использовать критерии подбора и расстановки сотрудников подразделений защиты информации;
У9	организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
У10	проводить инструктаж персонала по организации работы с конфиденциальной информацией;
У11	контролировать соблюдение персоналом требований режима защиты информации;
У12	осуществлять сбор информации,
У13	прогнозировать развитие событий и их последствия,
У14	прогнозировать развитие событий и их последствия,
У15	подготавливать аналитические и отчетные материалы,
У16	проводить аудит информационной безопасности инфраструктуры,
У17	осуществлять приём, выдачу и рассылку документов и сведений, связанных с организацией и проведением закупок;
У18	планировать закупки;
У19	разрабатывать извещение и документацию по закупкам;
У20	формировать команду проекта;

№	**Освоенные умения, усвоенные знания**
У21	определять цели и задачи проекта;
У22	формировать устав проекта;
У23	определять продолжительность проекта;
У24	определять ресурсы проекта;
У25	формировать стоимость проекта;
У26	рассчитывать эффективность проекта.
У27	тестировать информационные системы и сервера на наличие известных и широко распространенных уязвимостей.

Формой аттестации по профессиональному модулю является экзамен по профессиональному модулю. Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

2. СИСТЕМА КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ПРОГРАММЫ ПМ.05 «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

2.1. Формы промежуточной аттестации по ППССЗ при освоении профессионального модуля

Элементы модуля, профессиональный модуль	Формы промежуточной аттестации
МДК 05.01 «Основы управления информационной безопасностью»	Дифференцированный зачет
МДК 05.02 «Организация работы персонала с конфиденциальной информацией»	Дифференцированный зачет
МДК 05.03«Основы форензики»	Дифференцированный зачет
МДК.05.04. Организация закупки стандартного оборудования и ПО	Комплексный экзамен
МДК.05.05. Управление проектами ИБ	
Производственная практика	Зачет
ПМ	**Экзамен**

2.2. Организация контроля и оценки освоения программы ПМ

Итоговый контроль освоения вида профессиональной деятельности ПМ.05 «Управление информационной безопасностью» осуществляется на экзамене. Условием допуска к экзамену является положительная аттестация по МДК, учебной и производственной практикам.

Экзамен проводится в виде выполнения практического экзаменационного задания.

Условием положительной аттестации по ПМ.05 «Управление информационной безопасностью» (вид профессиональной деятельности освоен) на экзамене квалификационном является положительная оценка освоения всех профессиональных компетенций по всем контролируемым показателям. При отрицательном заключении хотя бы по одной из профессиональных компетенций принимается решение «вид профессиональной деятельности не освоен».

Промежуточный контроль освоения профессионального модуля осуществляется при проведении дифференцированного зачета по МДК.05.01 «Основы управления информационной безопасностью», дифференцированного зачета по МДК.05.02 «Организация работы персонала с конфиденциальной информацией», дифференцированного зачета по МДК.05.03 «Основы форензики», комплексного экзамена по МДК 05.04 «Организация закупки оборудования и ПО» и МДК 05.05 «Управление проектами» и зачета по учебной практике. Предметом оценки освоения МДК являются знания. Экзамен и комплексный экзамен по МДК проводятся по заранее подготовленным и утвержденным экзаменационным вопросам. Условием положительной аттестации является получение обучающимся на экзамене оценки «удовлетворительно», «хорошо», «отлично».

Предметом оценки по учебной практике является приобретение практического опыта по ведению учета и оформления бумажных и машинных носителей конфиденциальной информации, работе с информационными системами электронного документооборота. Контроль и оценка по учебной практике проводится на основе Аттестационного листа обучающегося с места прохождения практики.

Текущий контроль по МДК осуществляется в форме выполнения практических работ, устных зачетов.

3. КОМПЛЕКТ МАТЕРИАЛОВ ДЛЯ ОСВОЕНИЯ УМЕНИЙ И УСВОЕНИЯ ЗНАНИЙ, ОЦЕНКИ СФОРМИРОВАННОСТИ ОБЩИХ И ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ ПО ВИДУ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

3.1. Задания для оценки освоения теоретического курса профессионального модуля

3.1.1. Оценка освоения теоретического курса профессионального модуля по МДК.05.01

<table>
<tr><th rowspan="2">Дидактические единицы</th><th colspan="2">Формы контроля (наименование контрольной точки)</th></tr>
<tr><th>Текущая аттестация</th><th>Промежуточная аттестация</th></tr>
<tr><td>Тема 1.2. Политика безопасности автоматизированных систем</td><td>Практическая работа 2 Анализ политики ИБ предприятия</td><td rowspan="3">устные ответы на дифференцированном зачете</td></tr>
<tr><td rowspan="2">Тема 1.5. Основы управления рисками</td><td>Практическая работа 16 Количественная оценка рисков</td></tr>
<tr><td>Практическая работа 17 Качественная оценка рисков</td></tr>
</table>

Практическая работа № 3

Разработка политики ИБ предприятия

Задание

Для предприятия из работы №2 составьте политику информационной безопасности.

Политика должна содержать следующие пункты:

- Концепцию, которая определяет миссию и ключевые цели политики.
- Стандарты, то есть сами принципы обеспечения безопасности.
- Перечень конкретных действий, которые сотрудники должны совершать в процессе взаимодействия с конфиденциальными данными организации.
- Порядок работы с носителями данных.
- Правила доступа к корпоративным документам и другим важным ресурсам.
- Инструкции, касающиеся реализации методов защиты и применения принятых стандартов.
- Аварийные планы — порядок действий по реагированию и оперативному восстановлению информационных систем в случае непредвиденных обстоятельств (например, утечки, кибератаки, физических воздействий и т. д.).

Практическая работа № 16
Количественная оценка рисков

Задание
Проведите анализ следующих типов угроз ИБ для организации:
Умышленные несанкционированные действия людей.
Непредвиденные случайности.
Ошибки со стороны персонала.
Нарушение работоспособности оборудования, ошибки в ПО и отказы средств связи.
Первым этапом составляется перечень ИР. Для каждого ресурса перечисляются относящиеся к нему уязвимости и соответствующие им угрозы. Если существует уязвимость без связанной с ней угрозы, или существует угроза, не связанная с какими-либо уязвимостями, то рисков нет. Но и эти случаи следует предусмотреть.
Относящиеся к каждому типу негативных воздействий уровни рисков, соответствующих показателям ценности ресурсов, показателям угроз и уязвимостей, оцениваются при помощи таблицы, аналогичной таблице 1.

Показатель ценности ресурса (для каждого ресурса и угрозы)	**Уровень угрозы (вероятность ее осуществления)**								
	Низкий (Н)			**Средний (С)**			**Высокий (В)**		
	Уровень уязвимости			**Уровень уязвимости**			**Уровень уязвимости**		
	Н	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6

3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Таблица 1. Уровни рисков, соответствующие показателям ценности ресурсов, угроз и уязвимостей.

Количественный показатель риска определяется в шкале от 1 до 8 и вносится в соответствующую ячейку таблицы. Каждая строка в таблице определяет показатель ценности ресурса, а каждый столбец – степень опасности угрозы и уязвимости для ресурса. Например, ресурс имеет показатель ценности – 3, угроза имеет степень – «высокая», а уязвимость – «низкая». Показатель риска в этом случае будет равен – 5. Размер таблицы, учитывающей количество степеней опасности угроз, степеней опасности уязвимостей и категорий ценности ресурсов, может быть изменен в соответствии со спецификой конкретной организации.

Описанный подход определяется классификацией рассматриваемых рисков. После того, как оценивание рисков было выполнено первый раз, его результаты целесообразно сохранить, например, в базе данных. Эта мера в дальнейшем позволит легко повторить последующее оценивание рисков компании.

В матрице или таблице можно наглядно отразить связь между угрозами, негативными воздействиями и возможностями их реализации. Для этого нужно выполнить следующие шаги.

На первом шаге оценить показатель негативного воздействия по заранее определенной шкале, например, от 1 до 5, для каждого ресурса, которому угрожает опасность.

На втором шаге по заранее заданной шкале, например, также от 1 до 5, оценить вероятность реализации каждой угрозы.

На третьем шаге вычислить показатель риска путем перемножения чисел в колонках II и III, по которому и производится ранжирование угроз.

В этом примере (таблица 2) для наименьшего негативного воздействия и для наименьшей вероятности реализации выбран показатель 1.

I **Описание угрозы**	**II** **Показатель негативного воздействия**	**III** **Вероятность реализации угрозы**	**IV** **Показатель риска**	**V** **Ранг угрозы**
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Таблица 2. Ранжирование угроз.

Данная процедура позволяет сравнивать и ранжировать по приоритету угрозы с различными негативными воздействиями и возможностями реализации. В определенных случаях дополнительно могут потребоваться стоимостные показатели.

Оценка негативного воздействия угрозы

Эта задача решается при помощи оценивания двух значений: ценности ресурса и частоты повторяемости риска.

Сначала каждому ресурсу присваивается определенное значение, соответствующее потенциальному ущербу от воздействия угрозы. Такие показатели присваиваются ресурсу по отношению ко всем возможным угрозам. Суммированием баллов всех ресурсов анализируемой ИС определяется количественный показатель риска для всей системы.

Далее оценивается показатель частоты повторяемости риска. Частота зависит от вероятности возникновения угрозы и степени легкости, с которой может быть использована уязвимость (уровень уязвимости). В результате получается таблица, аналогичная таблице 3.

Уровень угрозы (вероятность ее осуществления)

Низкий			Средний			Высокий		
Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
Н	С	В	Н	С	В	Н	С	В
0	1	2	1	2	3	2	3	4

Таблица 3. Показатель частоты повторяемости риска.

Затем определяется показатель пары ресурс/угроза. На каждую пару ресурс/угроза составляется таблица, аналогичная таблице 4, в которой суммируются показатель ценности ресурса и показатель угрозы. Фактически таблица представляет собой матрицу, элементы которой равны сумме номеров строки и столбца конкретного элемента. Эту таблицу можно использовать в дальнейшем, для обоснования критичности того или иного ресурса – чем больше показатель пары ресурс/угроза, тем более критичен ресурс и на его защиту следует обратить больше внимания, на этапе управления рисками.

Показатель ценности ресурса	Показатель частоты повторяемости риска				
	0	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3=2+1	4	5	6
3	3	4	5=3+2	6	7
4	4	5	6	7	8

Таблица 4. Показатели пары ресурс/угроза.

На заключительном этапе суммируются все итоговые баллы по всем ресурсам ИС и формируется ее общий балл. Его можно использовать для выявления тех элементов системы, защита которых должна быть приоритетной.

Практическая работа № 17

Качественная оценка рисков

Задание

Проведите качественную оценку рисков информационной безопасности компании. Реализуйте алгоритм оценки либо вручную, либо используя средства программирования.

Входные данные алгоритма:

- информационные ресурсы;
- критичность ресурсов;
- угрозы, действующие на ресурсы;
- уязвимости, через которые реализуются угрозы;
- вероятность реализации угрозы через данную уязвимость;
- критичность реализации угрозы через данную уязвимость.

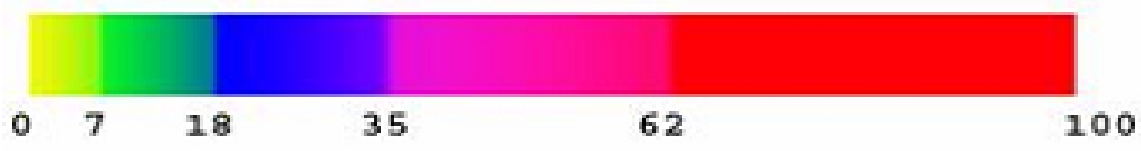
С точки зрения базовых угроз ИБ существует два режима работы алгоритма:

1. Одна базовая угроза (суммарная).
2. Три базовые угрозы.

Выбор шкалы для оценки риска и разбиение ее на уровни

При работе с алгоритмом используется числовая шкала от 0 до 100%. Шкалу разбивают максимум на 100 уровней. При разбиении шкалы на меньшее число уровней, каждый уровень занимает определенный интервал на шкале. Причем, возможно два варианта разделения:

– равномерное;



– логарифмическое.

Расчет рисков информационной безопасности

1. На первом этапе рассчитывается **уровень угрозы по уязвимости** (Th) на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

$$Th = \frac{ER}{100} \times \frac{P(V)}{100},$$

$$Th_{c,i,a} = \frac{ER_{c,i,a}}{100} \times \frac{P(V)_{c,i,a}}{100},$$

где $ER_{c,i,a}$ – критичность реализации угрозы (указывается в %), $P(V)_{c,i,a}$ – вероятность реализации угрозы через данную уязвимость по конфиденциальности, целостности и доступности (указывается в %).

Здесь вычисляется одно (Th) или три значения (Th_c, Th_i, Th_a) в зависимости от количества базовых угроз. Значение уровня угрозы по уязвимости лежит в отрезке [0, 1].

2. Чтобы рассчитать **уровень угрозы по всем уязвимостям** (CTh), через которые возможна реализация данной угрозы на ресурс, просуммируем полученные уровни угроз через конкретные уязвимости по следующим формулам.

Для режима с одной базовой угрозой:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th).$$

Для режима с тремя базовыми угрозами:

$$CTh_c = 1 - \prod_{i=1}^{n} (1 - Th_c),$$

$$CTh_i = 1 - \prod_{i=1}^{n} (1 - Th_i),$$

$$CTh_a = 1 - \prod_{i=1}^{n} (1 - Th_a).$$

Значение уровня угрозы по всем уязвимостям лежит в отрезке [0, 1].

3. Далее рассчитывается **общий уровень угроз по ресурсу** (CThR) с учетом всех угроз, действующих на ресурс.

Для режима с одной базовой угрозой:

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh).$$

Для режима с тремя базовыми угрозами:

$$CThR_c = 1 - \prod_{i=1}^{n} (1 - CTh_c),$$

$$CThR_i = 1 - \prod_{i=1}^{n} (1 - CTh_i),$$

$$CThR_a = 1 - \prod_{i=1}^{n} (1 - CTh_a).$$

Значение общего уровня угрозы лежит в отрезке [0, 1].

4. Итоговый **риск по ресурсу** (R), характеризующий возможные потери собственника ИС, связанные с реализацией некоторой угрозы через любую уязвимость, рассчитывается следующим образом.

Для режима с одной базовой угрозой:

$$R = CThR \times D,$$

где D – критичность ресурса. Для угроз нарушения целостности или доступности определяется заранее (в деньгах или уровнях в год), а в случае угрозы нарушения доступности ресурса (DoS – отказ в обслуживании) критичность ресурса в год рассчитывается по формуле:

$$D_{a/год} = D_{a/час} \times T,$$

где $D_{a/час}$ – критичность простоя ресурса в час, T – общее время простоя.

Для режима с тремя базовыми угрозами:

$$R_{c,i,a} = CThR_{c,i,a} \times D_{c,i,a},$$

$$R = (1 - (1 - \frac{R_c}{100})(1 - \frac{R_i}{100})(1 - \frac{R_a}{100})) \times 100,$$

где $D_{c,i,a}$ – критичность ресурса по каждой из трех угроз заданная в деньгах или уровнях в год.

5. Общий **риск по информационной системе** (CR) рассчитывается по следующим формулам.

Для режима с одной базовой угрозой:

$$CR = \sum_{i=1}^{n} R_i$$

– для случая оценки в деньгах;

$$CR = (1 - \prod_{i=1}^{n}(1 - \frac{R_i}{100})) \times 100$$

– для случая оценки в уровнях.

Для режима с тремя базовыми угрозами:

$$CR_{c,i,a} = \sum_{i=1}^{n} R_i,$$

$$CR = CR_c + CR_i + CR_a$$

– для случая оценки в деньгах;

$$CR_{a,c,i} = (1 - \prod_{i=1}^{n}(1 - \frac{R_i}{100})) \times 100,$$

$$CR = (1 - (1 - \frac{R_c}{100})(1 - \frac{R_i}{100})(1 - \frac{R_a}{100})) \times 100$$

– для случая оценки в уровнях. В обоих режимах подразумевается R_i – риск i-го ресурса, $CR_{c,i,a}$ – риск по ИС для каждого вида угроз.

6. Для расчета **эффективности введенной контрмеры** (E) необходимо заново пройти шаги 1-5 с учетом заданной контрмеры и определить значение двух рисков – риска без учета контрмеры (R_{old}) и риск с учетом заданной контрмеры (R_{new}) или с учетом того, что уязвимость закрыта.

Эффективность введения контрмеры рассчитывается по формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}}.$$

В результате работы алгоритма пользователь получает следующие данные:

1. Риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса.

2. Риск реализации суммарно по всем угрозам для ресурса.
3. Риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для ИС.
4. Риск реализации по всем угрозам для ИС.
5. Риск реализации по всем угрозам для ИС после задания контрмер.
6. Эффективность контрмеры.

3.1.2. Оценка освоения теоретического курса профессионального модуля по МДК.05.02

Дидактические единицы	Формы контроля (наименование контрольной точки)	
	Текущая аттестация	**Промежуточная аттестация**
Тема 2.3. Разрешительная система доступа к конфиденциальной информации	Устный зачет по теме 3.1.	Устные ответы на дифференцированном зачете
	Практическая работа № 6. Разработка номенклатуры должностей сотрудников, подлежащих оформлению на допуск к КИ	
	Практическая работа № 12. Подготовка памятки для персонала по организации работы с конфиденциальной информацией сотрудника при увольнении	
	Устный зачет по теме 3.3.	
Тема 2.6. Особенности работы с персоналом, владеющим конфиденциальной информацией	Практическая работа № 15. Решение ситуационных задач	
	Устный зачет по теме 3.4.	
	Устный зачет по теме 3.5	
	Практическая работа № 17. Разработка инструкции по соблюдению персоналом требований режима защиты конфиденциальной информации в процессе рекламной деятельности	
	Устный зачет по теме 3.6	

1. Устный зачет по темам 3.1.

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Охарактеризуйте понятие разрешительной системы доступа к конфиденциальной информации.
2. Каковы требования к разрешительной системе доступа к конфиденциальной информации.
3. Понятие допуска и доступа к конфиденциальной информации.
4. Положение о к разрешительной системе доступа к конфиденциальной информации. Назначение, структура.
5. Содержание основных разделов Положения о к разрешительной системе доступа к конфиденциальной информации.
6. Назначение экспертной комиссии по защите конфиденциальной информации, состав экспертной комиссии по защите конфиденциальной информации.
7. Функции экспертной комиссии по защите конфиденциальной информации.
8. Документы, сопровождающие работу экспертной комиссии по защите конфиденциальной информации.

Эталоны ответов: приведены в Учебном пособии по МДК.01.03 «Организация работы персонала с конфиденциальной информацией»

2. Практическая работа № 6
Разработка номенклатуры должностей сотрудников, подлежащих оформлению на допуск к КИ

Инструкция для обучающихся

Внимательно прочитайте задание. Составьте номенклатуру должностей сотрудников, подлежащих оформлению на допуск к КИ.

Время выполнения – 60 минут.

Задание:

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Разработайте и оформите номенклатуры должностей сотрудников, подлежащих оформлению на допуск к КИ **с учетом данных Вашей организации**.

При заполнении таблицы используйте следующие степени конфиденциальности: конфиденциально, строго конфиденциально.

Номенклатура должностей сотрудников,
подлежащих оформлению на допуск к конфиденциальной информации

Подразделение	Количество рабо-	Должность	Обоснование необходимо-	Количество лиц, подлежащих оформлению на доступ к КИ	Количество лиц, оформ-

	тающих		сти допуска	Вид КИ	Степень конфиденциальности 1	Степень конфиденциальности 2	Степень конфиденциальности …	ленных на доступ к КИ

В номенклатуре должны обязательно присутствовать грифы утверждения, согласования и подпись.

Вставьте проект номенклатуры.

Эталон ответа:

СОГЛАСОВАНО
Протокол заседания
экспертной комиссии по защите конфиденциальной информации
ООО «ДЕКОСП»
__.__.____ №__

УТВЕРЖДАЮ
Директор ООО «ДЕКОСП»
_____ В.С. Андреев
__.__.____

**Номенклатура должностей сотрудников,
подлежащих оформлению на допуск к конфиденциальной информации**

Подразделение	Количество работающих	Должность	Обоснование необходимости допуска	Количество лиц, подлежащих оформлению на доступ к КИ			Количество лиц, оформленных на доступ к КИ
				Вид КИ	Секретно	Совершенно секретно	
Отдел кадров	1	Менеджер по персоналу	Должностная инструкция	Персональные данные		1	1
Отдел разработки ПО	7	Разработчики ПО	Должностная инструкция	Секрет производства (ноу-хау)	7		7
Отдел разработки ПО	1	Руководитель отдела разработки ПО	Должностная инструкция	Сведения, касающиеся предмета договоров на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, хода их исполнения и полученных результатов, если иное не предусмотрено дого-	1		1

Подразделение	Количество работающих	Должность	Обоснование необходимости допуска	Количество лиц, подлежащих оформлению на доступ к КИ			Количество лиц, оформленных на доступ к КИ
				Вид КИ	Секретно	Совершенно секретно	
				ворами			
Отдел делопроизводства	1	Делопроизводитель	Должностная инструкция	Информация о содержании корпоративного договора, заключенного участниками непубличного общества	1		1
Бухгалтерия	1	Главный бухгалтер	Должностная инструкция	Сведения, содержащиеся в индивидуальных лицевых счетах в системе обязательного пенсионного страхования		1	1
Администрация	1	Директор	Должностная инструкция	Коммерческая тайна		1	1
Отдел безопасности	1	Руководитель отдела безопасности	Должностная инструкция	Сведения, связанные с аудитом организации		1	1
Отдел делопроизводства	1	Секретарь	Должностная инструкция	Коммерческая тайна	1		1
Отдел продаж	1	Менеджер по продажам	Должностная инструкция	Коммерческая тайна	1		1
Отдел продаж	1	Менеджер по продажам	Должностная инструкция	Персональные данные		1	1

3. Практическая работа № 12
«Подготовка памятки для персонала по организации работы с конфиденциальной информацией сотрудника при увольнении»

Инструкция для обучающихся

Внимательно прочитайте задание. Составьте памятки для персонала по организации работы с конфиденциальной информацией сотрудника при увольнении.

Время выполнения – 60 минут.

Задание:

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Используя материал лекций и ресурсы сети Интернет, составьте памятку для персонала по организации работы с конфиденциальной информацией сотрудника при увольнении.

Памятка должна содержать перечень действий, которые обязан выполнить сотрудник, который принял решение об увольнении.

Памятка должна быть оформлена общем бланке организации.

Требования по оформлению:
Основной текст - шрифт Times New Roman, 12 пт, междустрочный интервал 1,15, отступ красной строки 1, 25 см, выравнивание по ширине страницы.
Заголовок - шрифт Times New Roman, 12 пт, полужирный, междустрочный интервал 1,15, интервал после 24 пт, выравнивание по центру страницы.

Вставить памятку

Эталон ответа:

1. Перед увольнением с предприятия (переводом на работу, не связанную с конфиденциальной информацией), сотрудник обязан возвратить в службу безопасности предприятия (режимно-секретное подразделение) полученные ранее носители конфиденциальной информации (в том числе накопители на магнитных дисках), номерные металлические печати, ключи от сейфов и хранилищ.

2. Факт возврата подтверждается соответствующими подписями ответственных должностных лиц в обходном листе увольняемого сотрудника.

3. После заполнения обходного листа сотруднику выдается оформленная трудовая книжка и другие документы об увольнении. Получив трудовую книжку и произведя полный расчет с предприятием, увольняемый сотрудник возвращает в бюро пропусков (на контрольно-пропускной пункт при убытии с предприятия) пропуск для прохода на территорию и объекты предприятия.

4. При увольнении сотрудник обязан:

- написать заявление об увольнении с подробным раскрытием причины увольнения и желательно указанием места предполагаемой работы;
- передать заявление руководителю структурного подразделения для оформления и передачи секретарю-референту.
- передать секретарю-референту всех числящихся за сотрудником документов, баз данных, носителей информации, изделий, материалов, с которыми он рабо-

тал, проверка их комплектности, полноты и оформление приема в описи исполнителя или актом.

- сдать пропуск (идентификатор) для входа в рабочую зону, всех ключей и печатей, запрещение сотруднику входить в рабочее помещение с использованием знания шифра кодового замка.
- пройти беседу с сотрудником с целью напоминания сотруднику об обязательстве сохранения в тайне тех сведений, которые ему были доверены по службе в фирме, предупреждение сотрудника о запрещении использования этих сведений в интересах конкурента или в личных целях, выяснение причины увольнения и места новой работы.
- подписать обязательство о неразглашении им конфиденциальных сведений после увольнения.
- забрать трудовую книжку и расчет по заработной плате.

4. Устный зачет по теме 3.3.

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Охарактеризуйте понятие посетителя организации.
2. Назовите категории посетителей на уровне руководителя организации, приведите примеры.
3. Сформулируйте правила приема руководителем предприятия различных категорий посетителей.
4. Какова цель составления графика приема посетителей с точки зрения ИБ.
5. Кем, когда и как проверяется личность посетителя?
6. Каковы обязанности секретаря с точки зрения ИБ во время приема посетителей?
7. Каким образом могут быть организованы действия посетителя по окончании приема?
8. Каковы последствия нарушения посетителем требований защиты конфиденциальной информации?

Эталоны ответов: приведены в Учебном пособии по МДК.01.03 «Организация работы персонала с конфиденциальной информацией»

5. Практическая работа № 15 «Решение ситуационных задач»

Инструкция для обучающихся

Внимательно прочитайте задание. Ответьте на вопросы.

Время выполнения – 60 минут.

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Посмотрите внимательно на фотографию ниже:

3. Какие требования по обеспечению защиты конфиденциальной информации в ходе проведения совещаний/переговоров по конфиденциальным вопросам нарушены?

Ответ:

4. Какие действия необходимо предпринять сотрудникам подразделения безопасности после окончания совещания, показанного на фотографии, чтобы снизить риск утечки конфиденциальной информации?

Ответ:

Эталон ответа:

3. Какие требования по обеспечению защиты конфиденциальной информации в ходе проведения совещаний/переговоров по конфиденциальным вопросам нарушены?

Ответ:

1. Помещение должно быть без окон на улицу, если они есть, то должны быть затемнены и звукоизолированы.
2. У женщины ноутбук, который может быть средством шпионажа
3.Телефон лежит на столе, что может быть средством прослушки

4. Какие действия необходимо предпринять сотрудникам подразделения безопасности после окончания совещания, показанного на фотографии, чтобы снизить риск утечки конфиденциальной информации?

Ответ:

Осмотреть помещение на наличие стороннего оборудования
Проверить оборудование, которое было использовано во время переговоров
Опечатать переговорную и сдать под охрану

6. Устный зачет по теме 3.4.

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Какие совещания и переговоры называют конфиденциальными?
2. Что такое разглашение конфиденциальной информации? Каковы возможные причины и способы разглашения конфиденциальной информации?
3. Перечислите этапы проведения конфиденциальных совещаний и переговоров.
4. Каков порядок получения разрешения на проведение конфиденциальных совещаний и переговоров?
5. Каким образом организуются плановые и неплановые конфиденциальные совещания, проходящие без приглашения посторонних лиц?
6. Каким образом организуются плановые и неплановые конфиденциальные совещания, проходящие с участием посторонних лиц?
7. Кто несет ответственность за обеспечение защиты ценной информации в ходе конфиденциальных совещаний и переговоров?
8. Какие сотрудники участвуют в подготовке конфиденциального совещания?
9. Какие документы необходимо подготовить в процессе подготовки конфиденциального совещания?
10. Что не разрешается делать участникам конфиденциального совещания независимо от занимаемой должности и статуса во время конфиденциального совещания?

Эталоны ответов: приведены в Учебном пособии по МДК.01.03 «Организация работы персонала с конфиденциальной информацией»

7. Устный зачет по теме 3.5

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Какими нормативно-правовыми документами необходимо руководствоваться при передаче информации иностранному государству (организации)?

2. Какое подразделение осуществляет практическое выполнение задач по защите информации при международном сотрудничестве?
3. Каким локальным актом необходимо руководствоваться в ходе осуществления международного сотрудничества?
4. Какие вопросы регламентирует Инструкция о порядке работы с зарубежными партнерами?
5. Каковы обязанности руководителей подразделений, отвечающие за организацию работы по осуществлению международных связей?

Эталоны ответов: приведены в Учебном пособии по МДК.01.03 «Организация работы персонала с конфиденциальной информацией»

8. Практическая работа № 17
«Разработка инструкции по соблюдению персоналом требований режима защиты конфиденциальной информации в процессе рекламной деятельности»

Инструкция для обучающихся

Внимательно прочитайте задание. Разработайте проект Инструкции по соблюдению персоналом требований режима защиты конфиденциальной информации в процессе рекламной деятельности.

Время выполнения – 60 минут.

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Составьте и оформите инструкцию по защите конфиденциальной информации при работе с зарубежными партнерами **с учетом данных Вашей организации**.

При оформлении инструкции необходимо выполнить следующие требования:

1. Инструкция оформляется на бланке организации.
2. Инструкция должна быть утверждена руководителем организации
3. Инструкция должна быть согласована экспертной комиссией по защите конфиденциальной информацией.
4. Инструкция должна быть подписана составителем, которым является руководитель службы безопасности.
5. Инструкция должна обязательно содержать **лист ознакомления** сотрудника с инструкцией. Лист ознакомления должен располагаться в конце инструкции после реквизита подпись.

Правила оформления грифов и реквизитов приведены в ГОСТ 7.0.97-2016.
Текст ГОСТа можно прочитать здесь:
http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Ответ:

Эталон ответа:

СОГЛАСОВАНО
Протокол заседания
экспертной комиссии по защите конфиденциальной информации
ООО «ДЕКОСП»
__.__.____ №__

УТВЕРЖДАЮ
Директор
ООО «ДЕКОСП»
_____ В.С. Андреев
__.__.____

ИНСТРУКЦИЯ ПО РАБОТЕ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ В ПРОЦЕССЕ РЕКЛАМНОЙ ДЕЯТЕЛЬНОСТИ

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями законодательства Российской Федерации и учредительными документами ООО «ДЕЛОВЫЕ КОНСУЛЬТАЦИИ, САНКТ-ПЕТЕРБУРГ» (далее - Организация). Она предусматривает организационные и административные меры по защите конфиденциальной информации с целью предотвращения нанесения возможного экономического и морального ущерба Организации со стороны юридических и физических лиц, вызванного их неправомерными или неосторожными действиями путем присвоения или разглашения конфиденциальной информации.

1.2. Под конфиденциальной информацией понимается сведения, связанные с задачами, решаемыми Организацией в соответствии с учредительными документами, информация, связанная с управлением, финансами и другими сферами деятельности Организации, разглашение (искажение, передача, утечка и т.д.) которой может нанести ущерб интересам Организации. К сведениям, составляющим конфиденциальную информацию, относятся сведения, предусмотренные «Перечнем сведений, составляющих конфиденциальную информацию», утвержденным и введенным в действие приказом руководителя Организации № 1 от 15.01.2017

1.3. Разглашением конфиденциальной информации следует считать следующие действия сотрудника:

- доведение до сведения неуполномоченных лиц в устной, письменной, электронной или иной форме конфиденциальную информацию. Указанный факт может наступить в результате умысла сотрудника или по неосторожности, включая халатное отношение к своим обязанностям;
- использование конфиденциальной информации в процессе выполнения работы для другого предприятия, учреждения и организации или по заданию физического лица, иного субъекта предпринимательской деятельности без образования юридического лица;
- использование конфиденциальной информации в научной и педагогической деятельности;
- использование конфиденциальной информации в личных целях, не связанных с выполнением должностных обязанностей в Организации;
- использование конфиденциальной информации в ходе публичных выступлений, интервью и т.п.;
- иные действия сотрудника, в результате которых конфиденциальная информация, стала известна неуполномоченным лицам.

1.4. Не считаются разглашением конфиденциальной информации действия сотрудника, указанные в п.1.3. настоящей Инструкции, совершенные им в порядке и в случаях, предусмотренных законодательством Российской Федерации, во исполнение норматив-

ных актов Организации или договоров (соглашений) Организации с иными организациями или физическими лицами. Не считаются разглашением конфиденциальной информации действия сотрудника, совершенные им при наличии письменного разрешения или иного указания руководства Организации.

1.5. Меры по ограничению открытых публикаций конфиденциальной информации не могут быть использованы для сокрытия информации, связанной с:

- учредительными документами организации;
- документами, дающими право заниматься предпринимательской деятельностью (регистрационными удостоверениями, лицензиями, патентами и т.д.);
- сведениями о финансово-хозяйственной деятельности и иными сведениями, необходимыми для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему;
- документами о платежеспособности;
- сведениями о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;
- документами об уплате налогов и обязательных платежей;
- сведениями о загрязнении окружающей среды;
- сведениями о нарушении антимонопольного законодательства;
- сведениями о несоблюдении безопасных условий труда;
- сведениями о реализации продукции, причиняющей вред здоровью населения.

1.6. осуществлять следующие основные виды рекламной деятельности:

- наружная реклама, размещаемая на рекламных конструкциях в местах общего пользования (под рекламными конструкциями, в соответствии с Федеральным законом «О рекламе», понимаются щиты, стенды, строительные сетки, перетяжки, электронные табло и иные технические средства стабильного территориального размещения, монтируемые и располагаемые на внешних стенах, крышах и иных конструктивных элементах зданий, строений, сооружений или вне их, а также на остановочных пунктах движения общественного транспорта);
- реклама на телевидении и радио, а также в периодических печатных изданиях;
- реклама, распространяемая по сетям электросвязи и размещаемая в почтовых отправлениях;
- реклама на транспортных средствах (маршрутное такси, автобусы, электротранспорт) и с их использованием;
- реклама в ходе проведения конференций, симпозиумов, организуемых и проводимых вне предприятий;
- реклама, размещаемая в глобальных информационных сетях общего пользования;
- реклама в ходе проведения внутренних мероприятий с привлечением (приглашением, участием) представителей сторонних организаций и СМИ.

1.7. Ответственность за организацию работы с конфиденциальной информацией, разработку и осуществление необходимых мер по сохранности конфиденциальной информации руководитель Организации возлагает на руководителей структурных подразделений, соответствующих должностных лиц Службы безопасности, секретарей и системного администратора закрытой корпоративной компьютерной сети.

2. Порядок работы с конфиденциальной информацией при осуществлении рекламной деятельности

2.1. Основными направлениями защиты информации в ходе рекламной деятельности являются:

- подготовка и экспертиза материалов, предназначенных для использования в рекламной деятельности, на предмет отсутствия у них информации с ограниченным доступом;
- анализ материалов в процессе их подготовки рекламопроизводителем и рекламораспространителем к размещению в средствах рекламы;
- постоянный контроль порядка распространения и содержания распространенных рекламных материалов, независимо от способа, формы и периодичности их распространения.

2.2. При принятии руководителем фирмы решения о рекламировании деятельности фирмы, а также производимых ей товаров (оказываемых услуг), должностное лицо, назначенное ответственным за подготовку рекламных материалов и их передачу рекламопроизводителю и (или) рекламораспространителю, организует работу, направленную на предотвращение распространения в рекламе конфиденциальной информации.

2.3. Комплекс мероприятий по защите информации включает проведение комиссией фирмы экспертизы подготовленных к распространению материалов, анализ возможных форм, способов распространения рекламных материалов и непосредственное взаимодействие в процессе подготовки и распространения материалов с рекламопроизводителем и рекламораспространителем.

2.4. При проведении различных акции рекламного характера руководители фирмы, а также индивидуальные предприниматели и юридические лица (в том числе рекламопроизводители и рекламораспространители) обязаны представлять в антимонопольный орган информацию, необходимую для осуществления ими полномочий по государственному контролю над соблюдением законодательства Российской Федерации о рекламе, и обеспечивать его уполномоченным должностным лицам доступ к такой информации. Сведения, составляющие коммерческую, служебную и иную охраняемую законом тайну и полученные антимонопольным органом при осуществлении им своих полномочий, не подлежат разглашению, за исключением предусмотренных законодательством случаев.

2.5. При получении запроса из антимонопольного органа руководитель фирмы организует предоставление в установленный срок запрашиваемой информации и направление органу, приславшему запрос, письменного уведомления о невозможности ее распространения без согласия фирмы, являющейся обладателем информации.

Руководитель отдела безопасности _____ О.И. Комаров

С инструкцией ознакомлен: _____ _____ _____
(должность) (подпись) (фамилия, инициалы)

9. Устный зачет по теме 3.6

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Какие основные виды рекламной деятельности может осуществлять организация?
2. Каковы основные направлениями защиты информации в ходе рекламной деятельности?
3. Кто организует работу, направленную на предотвращение распространения в рекламе конфиденциальной информации?
4. Каковы функции комиссии, проводящей экспертизу материалов, используемых в процессе рекламной деятельности?
5. Какими средствами может осуществляться публикация материалов организации?
6. Каковы основные направлениями защиты информации в ходе публикаторской деятельности?
7. Перечислите основные мероприятия, направленные на исключение открытого опубликования информации с ограниченным доступом?
8. Кто несет ответственность за подготовку материалов к открытому опубликованию и соблюдение при этом требований по защите информации?
9. Каковы функции экспертной комиссии при подготовке и опубликовании материалов?

Эталоны ответов: приведены в Учебном пособии по МДК.01.03 «Организация работы персонала с конфиденциальной информацией»

3.1.3. Оценка освоения теоретического курса профессионального модуля по МДК.05.03

	Текущая аттестация	**Промежуточная аттестация**
Тема 3.4. Компьютерная форензика	Практическое занятие 12 Обнаружение инцидентов в ОС	Устные ответы на дифференцированном зачете
	Практическое занятие 13 Проведение расследования инцидента	
Тема 3.5 Сетевая форензика	Практическое занятие 14 Анализ сетевого трафика	
	Практическое занятие 15 Обнаружение действий нарушителя	

Практическая работа № 12 Обнаружение инцидентов в ОС
Задание:
Настройте auditd, обнаружьте и опишите произошедший инцидент.
auditd (сокращение от Linux Audit Daemon) — нативный инструмент предназначенный для мониторинга событий операционной системы и записи их в журналы событий, разрабатываемый и поддерживаемый компанией RedHat. Был создан для тесного взаимодействия с ядром операционной системы — во время своей работы наблюдает за системными вызовами и может записывать события — чтение, запись, выполнение, изменение прав - связанные с файлами ОС. Таким образом, с его помощью можно отслеживать практически любые события, происходящие в операционной системе.
Плюсы auditd:
- работает на низком уровне мониторинга — отслеживает системные вызовы и действия с файлами;
- имеет неплохой набор утилит в комплекте для удобства работы;
- постоянно развивается и обновляется;
- бесплатен и легко устанавливается.
Минусы auditd:
- большинство событий, возникающих при атаках характерных для конкретного приложения, практически невозможно отслеживать поскольку на уровне системных вызовов и работе с файлами трудно отличить взлом от нормальной работы приложения. Такие события лучше отслеживать на уровне самих приложений;
- auditd может замедлять работу ОС. Это связанно с тем, что подсистеме аудита необходимо проводить анализ системных вызовов;

- не слишком гибок в настройке правил;
- на данный момент это не лучший инструмент для работы с контейнерами.

Файлы конфигурации и синтаксис

Рассмотрим основные примеры настроек и параметров, которые будут использоваться далее. Более полное руководство по auditd вы можете найти здесь. Основную информацию можно найти в мануалах к auditd и его инструментам.

Файлы конфигурации хранятся в /etc/audit/. Правила желательно хранить в /etc/audit/rules.d/*.rules, по умолчанию доступ к этой директории только у root'a. Обратите внимание на то, что файл с правилами в этой директории должен иметь название *.rules, иначе auditd не прочитает его без явного указания. Если вы решили хранить правила в другом месте, то владелец файла должен быть root. Помимо этого рекомендую выставить группу файла root и права 600, чтобы никто кроме root'a не мог работать с файлом конфигурации auditd, т.к. зная что логируется, атакующий может избежать обнаружения. То же самое касается и файлов с правилами для других инструментов.

Правила для логирования можно добавлять следующими способами:
- записать его в файл(ы) /etc/audit/rules.d/<имя файла>.rules и перезапустить сервис;
- записать в файл по произвольному пути и указать его явно: auditctl -R <путь к файлу>;
- добавить правило утилитой auditctl [-A,-a] <правило>.

Синтаксис

Подробное описание синтаксиса на русском языке можно посмотреть здесь.

-D - удалить все правила. Обычно используется в начале файла, чтобы избежать неожиданностей;

-a [list,action],[action,list] - добавляет правило в конец списка правил. Списки и действия рассмотрим далее.

Основные варианты списков:

exit - Добавить правило к списку, отвечающему за точки выхода из системных вызовов. Этот список применяется, когда необходимо создать событие для аудита, привязанное к точкам выхода из системных вызовов.

exclude - Добавить правило к списку, отвечающего за фильтрацию событий определенного типа. Этот список используется, чтобы отфильтровывать ненужные события. Например, если вы не хотите видеть avc сообщения, вы должны использовать этот список. Тип сообщения задается в поле *msgtype*.

Варианты действий:

always - установить контекст аудита. Всегда заполнять его во время входа в системный вызов и всегда генерировать запись во время выхода из системного вызова;

never - аудит не будет генерировать никаких записей. Это может быть использовано для подавления генерации событий. Обычно необходимо подавлять генерацию вверху списка, а не внизу, т.к. событие инициируется на первом совпавшем правиле.

-A list,action - добавить правило в начало списка. Например, для удобство чтения правило находится ниже, чем должно быть по логике настроек, тогда можно использовать этот параметр.

-F [n=v | n!=v | n<v | n>v | n<=v | n>=v | n&v | n&=v] - задать поле сравнения для правила. Атрибуты поля следующие: объект, операция, значение. Вы можете задать до 64 полей сравнения в одной команде. Каждое новое поле должно начинаться с -F. Аудит будет генерировать запись, если произошло совпадение по всем полями сравнения. Допустимо использование одного из следующих 8 операторов: равно, не равно, меньше, больше, меньше либо равно, больше либо равно, битовая маска (n&v) и битовая проверка (n&=v). Битовая проверка выполняет операцию «and» над значениями и проверяет, равны ли они. Битовая маска просто выполняет операцию «and». Поля, оперирующие с идентификатором пользователя, могут также работать с именем пользователя — программа автоматиче-

ски получит идентификатор пользователя из его имени. То же самое можно сказать и про имя группы.
Поля сравнения и их описание:

- **a0, a1, a2, a3** - первые 4 аргумента системного вызова соответственно;
- **arch** - так как система ориентируется на номера (не названия) системных вызовов, а для многих системных вызовов номера отличаются для 32 и 64 разрядных систем, то необходимо указывать для какой архитектуры мы пишем правило;
- **auid** - ID пользователя, с которым он вошёл в систему. Системные сервисы, как правило, имеют auid=-1 (или 4294967295);
- **dir** - директория, за которой необходимо наблюдать. Будут залогированы и все события связанные с файлами и поддиректориями в указанной директории рекурсивно;
- **euid** - действительный идентификатор пользователя;
- **exe** - полный путь к исполняемому файлу. Может использоваться только с exit;
- **exit** - значение, возвращаемое системным вызовом при выходе;
- **key** - установка поля для фильтра. Добавляет поле с заданным именем в событие, что облегчает поиск событий в журналах;
- **msgtype** - тип события. Весь список событий можно посмотреть здесь;
- **path** - полный путь к файлу, за которым необходимо следить, может использоваться только с exit;
- **perm** - то же, что и параметр -p, будет рассмотрен ниже;
- **success** - если значение, возвращаемое системным вызовом, больше либо равно 0, данный объект будет равен «true/yes», иначе «false/no». При создании правила используйте 1 вместо «true/yes» и 0 вместо «false/no»;
- **uid** - идентификатор пользователя;

Вместо числовых идентификаторов пользователей можно указывать имена (www-data, mail, irc), таким образом вам не придется учитывать их числовые различия на разных серверах.
-p - [r|w|x|a] - описывает разрешение доступа файла за которым нужно следить: чтение, запись, выполнение или изменение прав доступа соответственно;
-w <path> - устанавливает наблюдение за директорией (рекурсивно) или файлом;
-W <path> - исключает наблюдение за указанной директорией или файлом.
Стоит упомянуть про встроенные инструменты анализа полученных событий: ausearch, aureport. С их помощью удобно тестировать правила "на месте". Много интересных примеров правил можно посмотреть здесь.
Общие принципы написания правил
Некоторые специалисты предпочитают писать правила максимально широкими, а логику фильтрации и обработки событий уже настраивать в подсистеме анализа событий, чтобы атакующий не знал какие его действия собираются и анализируются. На мой взгляд, у такого подхода есть недостаток: порождается большое количество событий из-за чего могут возникнуть проблемы с производительностью на серверах, где ведется сбор событий, и далее по цепочке архитектуры SIEM, особенно если источников логов много. Помимо этого в большой инфраструктуре сильно возрастает нагрузка по выявлению полезных событий среди общего потока в конечной точке.
Чтобы избежать случаев, когда атакующий может узнать, какие его действия анализируются, нужно установить мониторинг за файлом с правилами логирования таким образом, чтобы при чтении этого файла любым пользователем возникало событие, а также перечислить команды, позволяющие узнать правила без чтения файлов конфигурации такие как audictl -l.
На основе этих событий можно сделать алерты. Если логи передаются по сети, то, помимо установки наблюдения за доступом к правилам, необходимо настроить шифрование данных.

В независимости от того, какой подход будет выбран вами между ними есть много общего и, не смотря на то что в примерах далее почти вся логика будет настраиваться на источнике событий, фильтры/правила можно писать как на стороне источника событий, так и в подсистеме анализа событий (или даже на промежуточном этапе).
При написании правил auditd необходимо учитывать следующее:

1. Для каждого события отрабатывает лишь то подходящее правило, которое встретилось первым. Поэтому сначала пишутся фильтры и только потом правила. То же самое касается и выбора между несколькими правилами - выше размещать стоит то правило, которое важнее учитывать.
2. Писать правила лучше от частного к общему. Допустим, вы хотите журналировать действия в директории /etc/. Чтобы потом в логах не искать прикладными утилитами (grep, sed или средствами SIEM) все события, связанные, например, с ssh, sudoers, passwd и т.д., сначала указываете правила для мониторинга конкретных директорий/файлов в /etc/ и только после этого размещаете правило для самой директории /etc/.
3. В auditd есть преднастроенные правила и иногда возникают ситуации, когда они срабатывают и наши правила не учитываются. Поэтому каждое правило лучше предварительно тестировать отдельно.
4. Если вы хотите написать правила с целью выявления конкретного случая (атаки, ситуации), то лучше определить общее звено и написать правило для него. Так, например, для обнаружения запуска интерактивных шеллов можно использовать обращения к /dev/tty, /dev/pts/. Чем лучше вы понимаете как работает ваша операционная система, тем лучше. Используя такой подход, злоумышленнику станет тяжелее избежать обнаружения.
5. Для одного и того же действия с точки зрения пользователя может существовать несколько системных вызовов. Так для открытия файла могут использоваться: open, openat, creat, open_by_handle_at. Об этом стоит помнить, при создании правил на базе выборочных системных вызовов.
6. Если вы написали правило и видите множество ложных срабатываний, то, возможно, вместо написания множества фильтров, следует выбрать другой подход к определению события логирования.

Как тестировать правила
Прежде чем перейдем к конкретным примерам, стоит рассмотреть порядок тестирования будущих правил. В случае с инфраструктурой состоящей из нескольких серверов правила можно практически сразу применять, чего не скажешь о случаях, когда серверов десятки, сотни, или даже больше. Применение многих правил без предварительного тестирования способно вызвать перегрузку в разных местах: на самом сервере, на сети или в системе обработки событий. Чтобы избежать этого можно проводить тестирование следующим образом:

1. Проверка тестируемого правила на одном сервере. Чем ближе по составу установленного ПО сервер приближен к "боевой" среде, тем лучше. На этом этапе необходимо во-первых смоделировать условия, для которых написано правило, а во-вторых протестировать все возможные варианты поведения сервиса/приложения/пользователя, которые могут вызвать ложные срабатывания.
2. Проверка тестируемого правила в составе имеющихся других правил. На этом этапе проводим тесты и убеждаемся в том, что всё по-прежнему работает как задумано: другие правила могут перекрывать новое и наоборот.
3. Проверка нового набора правил на группе серверов. Снова, чем ближе к будущей инфраструктуре будут сервера по составу ПО, тем лучше. При необходимости этот этап можно повторять, увеличивая количество серверов.

4. Применение правил на всей инфраструктуре. Если по предыдущим пунктам вы убедились в "безопасности" нового набора, то можно применять его на всей инфраструктуре.

Если у вас большое количество серверов, то всегда стоит помнить о том, что какой-то участок вашей инфраструктуры может сработать не так как ожидалось и породить большое количество событий, поэтому пути решения возможных проблем лучше обдумать сразу.

Алгоритм тестирования правил

Для каждого правила в частности будем использовать следующий алгоритм:

1. Пробуем определить события для отслеживания по **формуле**:

AA - SA = IE

где AA - attacker's actions - набор действий атакующего, SA - service actions - набор действий сервиса в ходе его обычной деятельности, IE - incident events - события инцидента. Положительный результат (события инцидента) в формуле и будет основной целью для нас. Каждый набор действий состоит из системных вызовов и обращений к файлам. Эта формула может быть особенно полезна в случае с обнаружением инцидентов. Если явно выявить события инцидента не получается, то можно определить события, которые помогут при расследовании инцидента: обращения к важным файлам, выполнение команд и пр. На мой взгляд - хорошее правило то, для которого не нужно писать много фильтров и порождает события, по которым с высокой вероятностью можно сказать, что произошёл инцидент.

2. Пишем правило(а) для набора действий определенных в пункте 1.
3. Применяем правила: помимо событий которые мы хотим отслеживать, могут попадаться и другие события, о которых мы не знаем. Поэтому здесь необходимо создать как можно больше возможных вариантов легитимного поведения сервиса или событий, чтобы выявить действия сервиса, которые могут вызывать события по нашему правилу.
4. Пишем фильтры: если мы нашли такие события (п.3) то стоит подумать - можем ли мы от них избавиться. Писать фильтры желательно максимально точно, чтобы не "зацепить" лишних событий. В статье будет предложен вариант с написанием фильтров на хостах-источниках событий.
5. Моделируем ситуацию: создаём ситуацию, для которой написали правило и убеждаемся, что создаются необходимые события.

Модель угроз

Модель угроз для определения отслеживаемых событий, на мой взгляд, стоит рассматривать аналогично классическому: для обнаружения инцидента определяем все возможные способы взлома (вся информация, которая попадает на сервер), для расследования - вся информация, за которой мы хотим наблюдать. На этом этапе будет полезно устроить мозговой штурм среди коллег с целью составления способов взлома и/или проникновения на сервер в случае с обнаружением инцидента, а также наблюдаемых ресурсов для расследования. Затем можно в каждой из подгрупп провести ранжирование по важности отслеживаемых событий, после чего приступать к написанию правил. Подробную моделирование угроз выполнять не будем, т.к. это отдельная большая тема. Рассмотрим подгруппы подробнее.

Обнаружение инцидентов

С точки зрения логирования будем считать инцидентом ситуацию, при которой у атакующего появилась возможность выполнения команд и/или чтения файлов операционной системы. Для написания правил по обнаружению инцидентов, необходимо понять, каким образом он может вообще возникнуть. Поскольку для взлома сервера на него должны каким-то образом попасть данные от атакующего по сети, то в первую очередь необходимо определить пути попадания такой информации. Это любые сервисы, которые устанавливают соединения наружу и/или принимают входящие соединения. Причем чем раньше мы

сможем установить факт компрометации сервера, тем, очевидно, лучше. Основные способы выполнения команд на сервере:
- выполнение уже имеющихся исполняемых файлов (файлы директорий /bin/, /usr/bin/ и т.д.) — самый популярный способ. Например, атакующий получил доступ к командной оболочке напрямую или через имитацию шелла;
- выполнение команд через запись в файлы. Пример — планировщик задач cron. Если вы используете файлы, содержимое которых может быть выполнено как команды системой, то за ними необходим контроль;
- выполнение команд напрямую через системные вызовы — такой способ может применяться, например, в ходе "бинарных" атак: переполнения стека, кучи и т.д.
Что касается файлов, то наша задача определить те, что используется сервисом в обычной деятельности точно исключить такие события, поскольку в случае взлома сервиса, определить аномалию по отношению к таким файлам очень сложно.
Помимо вышеперечисленного, будем опираться на этапы проведения атаки:

1. Сканирование сервера.
   Злоумышленник производит обнаружение открытых портов на сервере извне.
2. Атака сервера, эксплуатация.
   На этом этапе злоумышленник каким-либо образом получает возможность чтения файлов, выполнению команд или системных вызовов на сервере. В этот условный этап будем относить все действия атакующего вплоть до момента выполнения любой первой команды и/или чтения первого файла, когда ему необходимо понять, что он смог добиться успеха в проведении атаки.
3. Взаимодействие с сервером, постэксплуатация.
   Вслед за взломом злоумышленник может попытаться закрепиться на сервере (оставить файл с шеллом, получить ssh-ключ и т.д.), найти информацию для продвижения вглубь инфраструктуры (поиск паролей, токенов в файлах, базах данных и т.д.).

Вы можете воспользоваться как уже имеющимися вариантами, например, mitre, так и использовать свой подход.

Расследование инцидентов

В этом случае нам необходима информация, которая поможет разобраться какие действия злоумышленник совершал после взлома: какие действия он выполнял, какие файлы читал и т.д. Принципы написания правил здесь будут отличаться от принципов при обнаружении инцидентов. В общем случае здесь необходимо устанавливать мониторинг за выполненными командами и важными с точки зрения безопасности файлами. Правила можно поделить на общие и частные. Общие - это те правила, которые подходят к любому серверу, вне зависимости от его назначения. Сюда можно отнести файлы конфигурации системы, пользователей и т.д. Частные - файлы и команды, характерные для сервера с конкретным назначением - веб-сервер, гипервизор и пр. Подробнее об этом рассмотрим в примере далее.

Основное отличие при работе по обнаружению инцидентов от расследования - стремление к созданию таких правил, события которых будут означать возникновение инцидента. Кратко: если возникло событие по правилу инцидента, то возник и сам инцидент.
В качестве примера возьмём сервер на котором есть http-сервис и ssh. Для каждого сервиса каждый этап взлома проведем через наш алгоритм. Проведём каждый сервис по этапам атаки через алгоритм, для каждого этапа будем применять формулу. Правила для расследования инцидентов рассмотрим отдельно позже, поскольку они подходят практически для любых видов сервисов. Все примеры ниже приведены на виртуальной ОС ubuntu 18.04, веб-сервер apache.
Будет полезен скрипт для автоматизации наших действий:

```
#!/bin/bash

killall -9 /sbin/auditd 2>/dev/null; \
systemctl stop auditd; \
systemctl stop apache2; \
sleep 2; \
rm /var/log/audit/audit.log*; \
systemctl start auditd; \
systemctl start apache2; \
auditctl -R /home/ubuntu/auditd/apache.rules > /dev/null 2>&1; \
auditctl -l; \
wc -l /var/log/audit/audit.log
```

Для быстрого завершения сначала убиваем процессы auditd, останавливаем сервисы auditd и apache2 (иногда без перезапуска apache2 правила по какой-то причине не применяются), удаляем все журналы логов, чтобы в поиске не выдавались старые результаты, запускаем сервисы, читаем правила из файла /home/ubuntu/auditd/apache.rules, проверяем список примененных правил, чтобы убедиться в что они работают и проверяем количество записей в файле лога аудита.

Файл /home/ubuntu/auditd/apache.rules:

```
-D
<тестируемые правила>
```

В первой строке **-D** используется для очистки существующих правил, которые мы могли забыть, чтобы избежать неожиданного поведения.

HTTP-Сервис

HTTP. Сканирование сервиса

1. На уровне системных вызовов мы можем определить лишь то сканирование, которое используют вызов connect, потому что тогда наш сервер использует accept во время установления соединения. В большинстве случаев мы не можем отличить соединение злоумышленника, поскольку такое соединение ни чем не отличается от обычных пользователей. Однако, если у вас такой веб-сервер находится внутри инфраструктуры и есть ограниченное количество сетевых устройств, которые могут к нему подключаться, то такое правило может иметь смысл в случае определения белого списка сетевых устройств устанавливающих соединение.
2. Правило для auditd будет выглядеть следующим образом:

-a **exit**,always -S accept -S accept4 -F exe=/usr/sbin/apache2 -k accept

Читается как: всегда на выходе из системных вызовов accept или accept4 для исполняемого файла /usr/sbin/apache2 логировать события и добавлять к ним метку accept.

3. Понятно, что любой соединение от клиента будет вызывать появление таких событий, смоделируем сканирование:

```
nc -z localhost 80
```

Результат:

```
$ ausearch -k apache_accept -i
----
type=PROCTITLE msg=audit(12.08.2021 16:05:29.654:395) : proctitle=/usr/sbin/apache2 -k
start
type=SOCKADDR msg=audit(12.08.2021 16:05:29.654:395) : saddr={ fam=inet6
laddr=::ffff:127.0.0.1 lport=37112 }
type=SYSCALL msg=audit(12.08.2021 16:05:29.654:395) : arch=x86_64 syscall=accept4 suc-
cess=yes exit=11 a0=0x4 a1=0x7ffd4ca5c800 a2=0x7ffd4ca5c7e0 a3=0x80000 items=0
ppid=5041 pid=5050 auid=unset uid=www-data gid=www-data euid=www-data suid=www-
data fsuid=www-data egid=www-data sgid=www-data fsgid=www-data tty=(none) ses=unset
comm=apache2 exe=/usr/sbin/apache2 key=apache_accept
```

Видим, что поле по которому мы хоть как-то могли бы фильтровать события это saddr, однако такого поля в опциях у auditd нет и такое возможно вспомогательными средствами: go-audit, elk;

4. Поскольку фильтры, которые были бы нам полезны, написать не можем, пропускаем этот шаг.

Результат: в широком смысле мы можем отслеживать все входящие сетевые соединения, а логику для написания алертов необходимо дополнительно настраивать. В целом - это не лучшее правило для создания событий с целью обнаружения инцидентов, однако в определенных случаях такие правила могут быть полезны.

HTTP. Атака сервиса

1. На данном этапе злоумышленник каким-либо образом получил возможность читать файлы ОС или выполнять команды. Можем предположить, что действия атакующего будут затрагивать файлы в директориях /bin/, /usr/bin/, часто пытаются прочитать файл /etc/passwd как в ходе автоматизированной так и при ручной атаках. Действия веб-сервера в большинстве случаев находится в директории /var/www/. Таким образом, возникает идея логировать действия для пользователя www-data везде, кроме директории /var/www.
2. Далее пишем правила для наших предположений:

```
-a never,exit -F dir=/var/www/ -F uid=www-data
-w / -F uid=www-data -k apache_alert
```

3. Затем переходим к тестированию. После выполнения скрипта check.sh, обратимся к одной из страниц веб-сервера. Сделаем файл /var/www/html/test.php с содержимым:

```
<?php phpinfo(); >?
```

После этого загружаем через браузер этот файл, останавливаем и запускаем службу:
Логи
Как видим, в логах присутствуют записи, которые мы не ожидали увидеть.

4. Пишем фильтры. Из получившихся событий мы видим, что пользователь www-data обращается к файлам директории /usr/share/zoneinfo/. Поскольку никакой ценной информации с точки зрения безопасности в этой директории не содержится, мы можем написать фильтр, чтобы избавиться от этих событий:

```
-a never,exit -F dir=/usr/share/zoneinfo/ -F uid=www-data
```

Тестируем снова, убеждаемся, что эти события пропали из журналов и других "лишних" событий не присутствует. Можем переходить к моделированию поведения атакующего.

5. Смоделируем условия, при которых атакующий смог воспользоваться уязвимостью LFI или загрузить веб-шелл и воспользоваться какой-то командой.

В директории /var/www/html/ разместим файл read_passwd.php с содержимым:

```
<?php
$myfile = fopen("/etc/passwd", "r") or die("Unable to open file!");
echo fread($myfile,filesize("/etc/passwd"));
fclose($myfile);
?>
```

И еще один shell.php который имитирует простейший веб-шелл:

```
<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>
```

Получим через браузер сначала read_file.php и выполним поиск по логам:

```
$ ausearch -k apache_alert -i
----
type=PROCTITLE msg=audit(12.08.2021 23:12:08.373:688) : proctitle=/usr/sbin/apache2 -k start
type=PATH msg=audit(12.08.2021 23:12:08.373:688) : item=0 name=/etc/passwd inode=264156 dev=08:01 mode=file,644 ouid=root ogid=root rdev=00:00 nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
```

type=CWD msg=audit(12.08.2021 23:12:08.373:688) : cwd=/var/www/html
type=SYSCALL msg=audit(12.08.2021 23:12:08.373:688) : arch=x86_64 syscall=openat success=yes exit=12 a0=0xffffff9c a1=0x7ffea2903630 a2=O_RDONLY a3=0x0 items=1 ppid=3410 pid=3419 auid=**unset** uid=www-data gid=www-data euid=www-data suid=www-data fsuid=www-data egid=www-data sgid=www-data fsgid=www-data tty=(none) ses=**unset** comm=apache2 exe=/usr/sbin/apache2 key=apache_alert
После этого в браузере выполним запрос:
http://192.168.0.101/shell.php?cmd=ls
И выполнив поиск по логам, увидим, что добавились события:
---
type=PROCTITLE msg=audit(12.08.2021 23:14:57.566:707) : proctitle=sh -c ls
type=PATH msg=audit(12.08.2021 23:14:57.566:707) : item=0 name=/etc/ld.so.cache inode=265858 dev=08:01 mode=file,644 ouid=root ogid=root rdev=00:00 nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(12.08.2021 23:14:57.566:707) : cwd=/var/www/html
type=SYSCALL msg=audit(12.08.2021 23:14:57.566:707) : arch=x86_64 syscall=openat success=yes exit=3 a0=0xffffff9c a1=0x7feec9ccbea8 a2=O_RDONLY|O_CLOEXEC a3=0x0 items=1 ppid=3422 pid=3433 auid=**unset** uid=www-data gid=www-data euid=www-data suid=www-data fsuid=www-data egid=www-data sgid=www-data fsgid=www-data tty=(none) ses=**unset** comm=sh exe=/bin/dash key=apache_alert
---
type=PROCTITLE msg=audit(12.08.2021 23:14:57.562:706) : proctitle=sh -c ls
type=PATH msg=audit(12.08.2021 23:14:57.562:706) : item=1 name=/lib64/ld-linux-x86-64.so.2 inode=3156086 dev=08:01 mode=file,755 ouid=root ogid=root rdev=00:00 nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(12.08.2021 23:14:57.562:706) : item=0 name=/bin/sh inode=1966114 dev=08:01 mode=file,755 ouid=root ogid=root rdev=00:00 nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(12.08.2021 23:14:57.562:706) : cwd=/var/www/html
type=EXECVE msg=audit(12.08.2021 23:14:57.562:706) : argc=3 a0=sh a1=-c a2=ls
type=SYSCALL msg=audit(12.08.2021 23:14:57.562:706) : arch=x86_64 syscall=execve success=yes exit=0 a0=0x7f5978e1de1a a1=0x7ffea29045e0 a2=0x7ffea29073d8 a3=0x1 items=2 ppid=3422 pid=3433 auid=**unset** uid=www-data gid=www-data euid=www-data suid=www-data fsuid=www-data egid=www-data sgid=www-data fsgid=www-data tty=(none) ses=**unset** comm=sh exe=/bin/dash key=apache_alert
....
Всё работает как было задумано.
Результат: такими правилами мы обнаружим любое обращение к файлам, которые не используются веб-сервером в рамках привычной своей деятельности и могут являться целью злоумышленника. В приведенном примере использовался веб-сервер без каких-либо приложений, фильтров может быть больше, однако, если вам удастся подобным образом написать правила, то многие наиболее критичные виды веб-уязвимостей (RCE, LFI, SSTI, XXE и т.д.) при выполнении команд в системе или чтении файлов могут быть обнаружены в момент их реализации.
В случае, если исключений слишком много. можно пойти другим путем и написать правила для наблюдения только за наиболее важными директориями в системе. Например:
```
# dirs from PATH var
-w /bin -F uid=www-data -k apache_alert
-w /usr/local/sbin -F uid=www-data -k apache_alert
-w /usr/local/bin -F uid=www-data -k apache_alert
-w /usr/sbin -F uid=www-data -k apache_alert
-w /usr/bin -F uid=www-data -k apache_alert
```

-w /sbin -F uid=www-data -k apache_alert

-w /etc -F uid=www-data -k apache_alert
Таким образом при обращении пользователя веб-сервера к исполняемым файлам системы будут созданы соответствующие события.

HTTP. Постэксплуатация

Поскольку на предыдущем шаге мы установили наблюдение за почти всеми возможными ... непокрытое поле для злоумышленника остаётся только в директории /var/www/. Можем предположить, что он может попытаться записать новый файл с функционалом для веб-приложения или изменить существующий для реализации новой логики. Если у вас приложение не создаёт динамических страниц, то для обнаружения изменений в существующих файлах веб-приложения можно написать следующие правила:
-w /var/www/ -p wa -F uid=www-data -k apache_file_change
Тогда для всех случаев когда файлы открываются для записи или изменения прав веб-сервером будут записаны события. Это правило необходимо разместить над фильтрами. Итоговый набор правил может выглядеть так:
-D
-w /var/www/ -p wa -F uid=www-data -k apache_file_change
-a never,exit -F dir=/usr/share/zoneinfo/ -F uid=www-data
-a never,exit -F dir=/var/www/ -F uid=www-data
-w / -F uid=www-data -k apache_alert
SSH сервис

Немного забегая вперёд, стоит отметить, что правила по обнаружению инцидентов возникающих через ssh-сервис очень схожи с правилами по расследованию инцидентов, поэтому многие правила из этого раздела можно использовать и при расследовании инцидентов. Это связано со спецификой самого ssh-сервиса.

SSH. Сканирование сервиса

Данный этап идентичен с этапом для HTTP-сервиса, поэтому его пропускаем.

SSH. Атака сервиса

Учитывая назначение сервиса, объеденим атаку и постэксплуатацию - поскольку взлом самого сервиса маловероятен, сфокусируемся на случае, когда злоумышленник получил доступ к сервису "популярным" способом - узнал пароль или ключ.

1. Определим действия. Рассматривать атакую перебор учетных данных сервиса не будем, т.к. есть более удобные инструменты для отслеживания таких атак, однако стоит отметить, что по умолчанию в журналы аудиты попадают все события связанные с попытками логина и аутентификации. Пример неудачной попытки ввода учетных данных:

time->Fri Aug 13 14:45:27 2021
type=USER_LOGIN msg=audit(1628855127.918:860): pid=8622 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct=28756E6B6E6F776E207573657229 exe="/usr/sbin/sshd" hostname=? addr=192.168.0.104 terminal=sshd res=failed'
---
time->Fri Aug 13 14:45:27 2021
type=USER_LOGIN msg=audit(1628855127.918:861): pid=8622 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct=28696E76616C6964207573657229 exe="/usr/sbin/sshd" hostname=? addr=192.168.0.104 terminal=sshd res=failed'
---
time->Fri Aug 13 14:45:30 2021
type=USER_AUTH msg=audit(1628855130.974:862): pid=8622 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="testy" exe="/usr/sbin/sshd" hostname=192.168.0.104 addr=192.168.0.104 terminal=ssh res=failed'
---

time->Fri Aug 13 14:45:30 2021
type=USER_LOGIN msg=audit(1628855130.974:863): pid=8622 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct=28696E76616C6964207573657229 exe="/usr/sbin/sshd" hostname=? addr=192.168.0.104 terminal=sshd res=failed'
SSH изначально предполагает подключение пользователей и предоставление им возможности выполнять команды, поэтому обнаружение подозрительной активности становится весьма нетривиальной задачей.
В зависимости от предназначения сервера, наборы подозрительных действий могут отличаться. Так если сервер предназначен, например, для веб-разработки, то маловероятно, что пользователям нужны утилиты связанные с дампом трафика. Можно предположить, что злоумышленника будет интересовать сбор сведений о системе, поиск ценных данных о проекте (компании), повышение привилегий в системе. Для начала можно пройтись по спискам Linux Privilege Escalation, ознакомиться с основными способами сбора информации там и настроить правила для них. Затем, исходя из специфики сервера, необходимо добавить дополнительные правила.

2. Поскольку правил может быть очень много, рассмотрим основные. Много полезных примеров для этого раздела я нашёл здесь. Интересно, что auditd с собой несёт тоже несколько примеров наборов правил, есть даже для pci-dss-v31:

$ ls /usr/share/doc/auditd/examples/rules
10-base-config.rules 12-cont-fail.rules 21-no32bit.rules 30-nispom.rules.gz 31-privileged.rules 41-containers.rules 70-einval.rules README-rules
10-no-audit.rules 12-ignore-error.rules 22-ignore-chrony.rules 30-pci-dss-v31.rules.gz 32-power-abuse.rules 42-injection.rules 71-networking.rules
11-loginuid.rules 20-dont-audit.rules 23-ignore-filesystems.rules 30-stig.rules.gz 40-local.rules 43-module-load.rules 99-finalize.rules

Для каждого события будем добавлять строку "susp_", по этому ключу можно будет найти любые подозрительные действия в системе, а также удобно настраивать поиск в подсистеме анализа.
Начнём с логирования действий над самим инструментом:
-w /etc/audit/ -p wa -k susp_auditconfig
-w /etc/audisp/ -p wa -k susp_audispconfig
-w /sbin/auditctl -p x -k susp_audittools
-w /sbin/auditd -p x -k susp_audittools
-w /usr/sbin/augenrules -p x -k susp_audittools
-w /var/log/audit/ -k susp_auditlog
Запись или изменение прав файлов планировщика задач:
-w /etc/cron -p wa -k cron_change
-w /etc/crontab -p wa -k cron_change
-w /etc/cron.allow -p wa -k cron_change
-w /etc/cron.d -p wa -k cron_change
-w /etc/cron.deny -p wa -k cron_change
-w /etc/cron.daily -p wa -k cron_change
-w /etc/cron.hourly -p wa -k cron_change
-w /etc/cron.monthly -p wa -k cron_change
-w /etc/cron.weekly -p wa -k cron_change
-w /etc/anacrontab -p wa -k cron_change
-w /var/spool/cron -p wa -k cron_change
-w /var/spool/cron/crontabs/root -p wa -k cron_change
Интересным кажется вариант с логированием выполнения команды sudo всеми пользователями, кроме того (тех), кому такие права не выданы:
-w /usr/bin/sudo -F auid!=<имя пользователя> -k susp_sudo
Важно наблюдать за работой сетевых утилит:

-w /sbin/iptables -p x -k susp_netutil
-w /sbin/ip6tables -p x -k susp_netutil
-w /sbin/ifconfig -p x -k susp_netutil
-w /usr/sbin/arptables -p x -k susp_netutil
-w /usr/sbin/ebtables -p x -k susp_netutil
-w /sbin/xtables-nft-multi -p x -k susp_netutil
-w /usr/sbin/nft -p x -k susp_netutil
Особый интерес представляют события, связанные с различными нарушениями доступа пользователей: при чтении, записи, изменении файлов:
File Access
Unauthorized Access (unsuccessful)
-a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k file_access
-a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k file_access
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k file_access
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k file_access

Unsuccessful Creation
-a always,exit -F arch=b32 -S creat,link,mknod,mkdir,symlink,mknodat,linkat,symlinkat -F exit=-EACCES -k file_creation
-a always,exit -F arch=b64 -S mkdir,creat,link,symlink,mknod,mknodat,linkat,symlinkat -F exit=-EACCES -k file_creation
-a always,exit -F arch=b32 -S link,mkdir,symlink,mkdirat -F exit=-EPERM -k file_creation
-a always,exit -F arch=b64 -S mkdir,link,symlink,mkdirat -F exit=-EPERM -k file_creation

Unsuccessful Modification
-a always,exit -F arch=b32 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EACCES -k file_modification
-a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EACCES -k file_modification
-a always,exit -F arch=b32 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EPERM -k file_modification
-a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EPERM -k file_modification
Обратите внимание, что правила написаны для системных вызовов разных архитектур отдельно.
Как показала практика, у таких правил часто возникают ложные срабатывания, в таким случае их можно изменить, добавив срабатывание только на пользовательские действия. После опции -S <системный вызов> необходимо добавить:
-F auid>=1000 -F auid!=-1
Результат: SSH-сервис, на мой взгляд, один из самых сложных сервисов для обнаружения инцидента при помощи auditd, поэтому для него должны быть использованы надежные средства защиты, которые не позволят злоумышленнику получить доступ к серверу, . Созданные на этом этапе правила во многом могут быть использованы для расследования инцидентов о чем будет сказано далее.

Практическая работа № 13 Проведение расследования инцидента
Задание:

Изучите выданные дампы памяти и снимки состояния ОС. Обнаружьте инцидент и дайте полное описание с указанием времени и используемых нарушителем средств.
Оформите отчет об инциденте в правильном формате.

Практическая работа № 14 Анализ сетевого трафика

Задание:

Изучите выданные дампы сетевой памяти. Проведите анализ сетевого трафика и выявите флаги в каждом. Заполните таблицу.

Название файла	**Флаг**
1	**Flag(wefgjejnwuuw)**
2	**Flag(13jgvivie35ocww)**
3	**Flag([pq-[kr4mm88)**

Практическая работа № 15 Обнаружение действий нарушителя

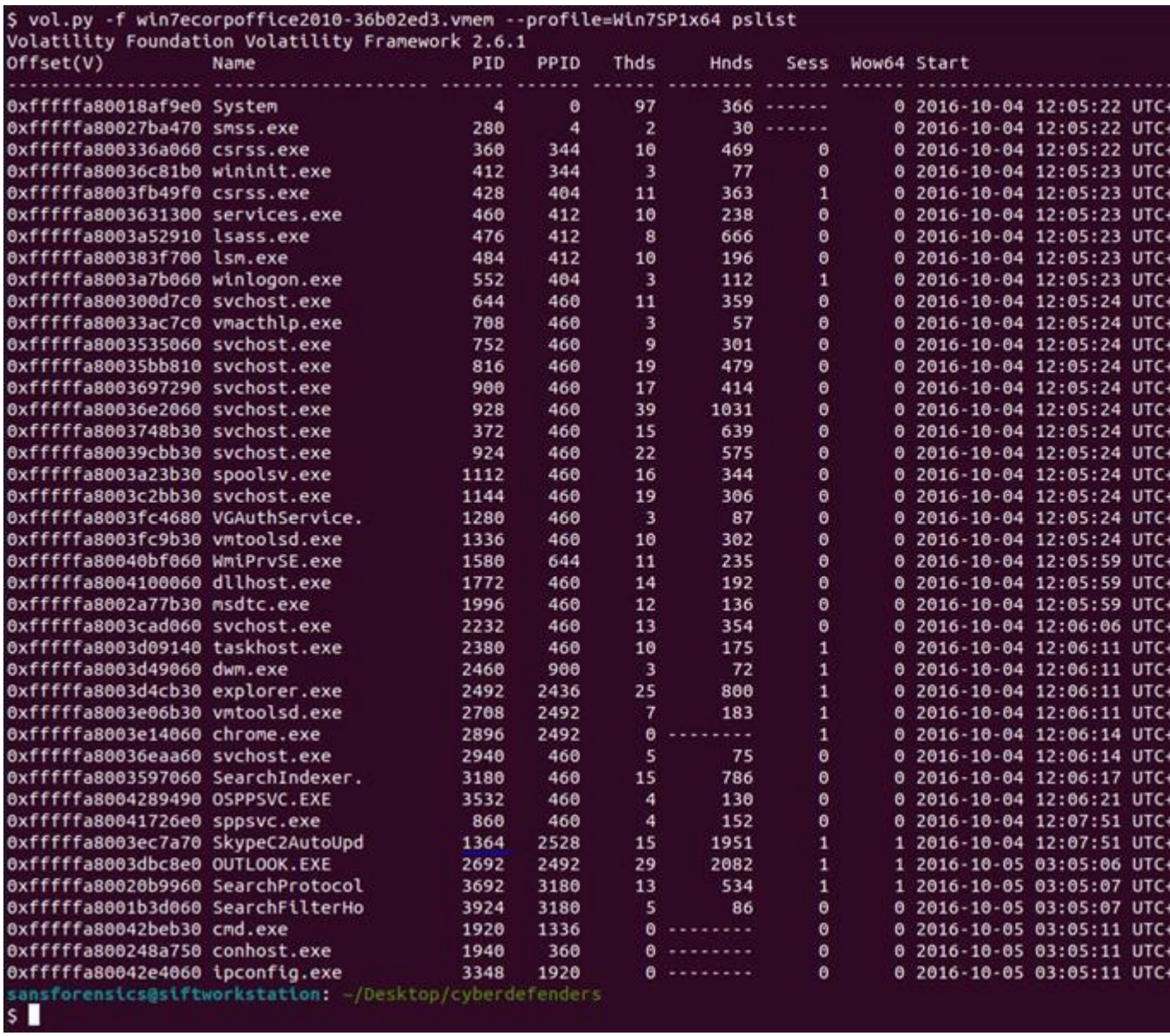
Задание:

Изучите выданные дампы сетевой памяти. Опишите полную последовательность действий нарушителя, какие протоколы были использованы, изучите последствия и дайте рекомендации по устранению.

Расследование в первом файле виртуальной машины.

Вначале посмотрим, какие процессы запущены на первом скомпрометированном хосте при помощи плагина **pslist**(Рисунок 1). Для этого, выполним команду:

vol.py pslist



```
$ vol.py -f win7ecorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
------------------ -------------------- ------ ------ ------ -------- ------ ------ ----------------------
0xfffffa80018af9e0 System                    4      0     97      366 ------      0 2016-10-04 12:05:22 UTC
0xfffffa80027ba470 smss.exe                280      4      2       30 ------      0 2016-10-04 12:05:22 UTC
0xfffffa800336a060 csrss.exe               360    344     10      469      0      0 2016-10-04 12:05:22 UTC
0xfffffa80036c81b0 wininit.exe             412    344      3       77      0      0 2016-10-04 12:05:23 UTC
0xfffffa8003fb49f0 csrss.exe               428    404     11      363      1      0 2016-10-04 12:05:23 UTC
0xfffffa8003631300 services.exe            460    412     10      238      0      0 2016-10-04 12:05:23 UTC
0xfffffa8003a52910 lsass.exe               476    412      8      666      0      0 2016-10-04 12:05:23 UTC
0xfffffa800383f700 lsm.exe                 484    412     10      196      0      0 2016-10-04 12:05:23 UTC
0xfffffa8003a7b060 winlogon.exe            552    404      3      112      1      0 2016-10-04 12:05:23 UTC
0xfffffa800300d7c0 svchost.exe             644    460     11      359      0      0 2016-10-04 12:05:24 UTC
0xfffffa80033ac7c0 vmacthlp.exe            708    460      3       57      0      0 2016-10-04 12:05:24 UTC
0xfffffa8003535060 svchost.exe             752    460      9      301      0      0 2016-10-04 12:05:24 UTC
0xfffffa80035bb810 svchost.exe             816    460     19      479      0      0 2016-10-04 12:05:24 UTC
0xfffffa8003697290 svchost.exe             900    460     17      414      0      0 2016-10-04 12:05:24 UTC
0xfffffa80036e2060 svchost.exe             928    460     39     1031      0      0 2016-10-04 12:05:24 UTC
0xfffffa8003748b30 svchost.exe             372    460     15      639      0      0 2016-10-04 12:05:24 UTC
0xfffffa80039cbb30 svchost.exe             924    460     22      575      0      0 2016-10-04 12:05:24 UTC
0xfffffa8003a23b30 spoolsv.exe            1112    460     16      344      0      0 2016-10-04 12:05:24 UTC
0xfffffa8003c2bb30 svchost.exe            1144    460     19      306      0      0 2016-10-04 12:05:24 UTC
0xfffffa8003fc4680 VGAuthService.         1280    460      3       87      0      0 2016-10-04 12:05:24 UTC
0xfffffa8003fc9b30 vmtoolsd.exe           1336    460     10      302      0      0 2016-10-04 12:05:24 UTC
0xfffffa80040bf060 WmiPrvSE.exe           1580    644     11      235      0      0 2016-10-04 12:05:59 UTC
0xfffffa8004100060 dllhost.exe            1772    460     14      192      0      0 2016-10-04 12:05:59 UTC
0xfffffa8002a77b30 msdtc.exe              1996    460     12      136      0      0 2016-10-04 12:05:59 UTC
0xfffffa8003cad060 svchost.exe            2232    460     13      354      0      0 2016-10-04 12:06:06 UTC
0xfffffa8003d09140 taskhost.exe           2380    460     10      175      1      0 2016-10-04 12:06:11 UTC
0xfffffa8003d49060 dwm.exe                2460    900      3       72      1      0 2016-10-04 12:06:11 UTC
0xfffffa8003d4cb30 explorer.exe           2492   2436     25      800      1      0 2016-10-04 12:06:11 UTC
0xfffffa8003e06b30 vmtoolsd.exe           2708   2492      7      183      1      0 2016-10-04 12:06:11 UTC
0xfffffa8003e14060 chrome.exe             2896   2492      0 --------      1      0 2016-10-04 12:06:14 UTC
0xfffffa80036eaa60 svchost.exe            2940    460      5       75      0      0 2016-10-04 12:06:14 UTC
0xfffffa8003597060 SearchIndexer.         3180    460     15      786      0      0 2016-10-04 12:06:17 UTC
0xfffffa8004289490 OSPPSVC.EXE            3532    460      4      130      0      0 2016-10-04 12:06:21 UTC
0xfffffa80041726e0 sppsvc.exe              860    460      4      152      0      0 2016-10-04 12:07:51 UTC
0xfffffa8003ec7a70 SkypeC2AutoUpd         1364   2528     15     1951      1      1 2016-10-04 12:07:51 UTC
0xfffffa8003dbc8e0 OUTLOOK.EXE            2692   2492     29     2082      1      1 2016-10-05 03:05:06 UTC
0xfffffa80020b9960 SearchProtocol         3692   3180     13      534      1      1 2016-10-05 03:05:07 UTC
0xfffffa8001b3d060 SearchFilterHo         3924   3180      5       86      0      0 2016-10-05 03:05:07 UTC
0xfffffa80042beb30 cmd.exe                1920   1336      0 --------      0      0 2016-10-05 03:05:11 UTC
0xfffffa800248a750 conhost.exe            1940    360      0 --------      0      0 2016-10-05 03:05:11 UTC
0xfffffa80042e4060 ipconfig.exe           3348   1920      0 --------      0      0 2016-10-05 03:05:11 UTC
sansforensics@siftworkstation: ~/Desktop/cyberdefenders
$
```

Рисунок 1 – список запущенных на хосте процессов в режиме реального времени.

Давайте более детально посмотрим на дерево родительских и дочерних процессов, а также директории, откуда процесс был запущен (плагин **pstree** с флагом **-v**). Результат на рисунке 2.

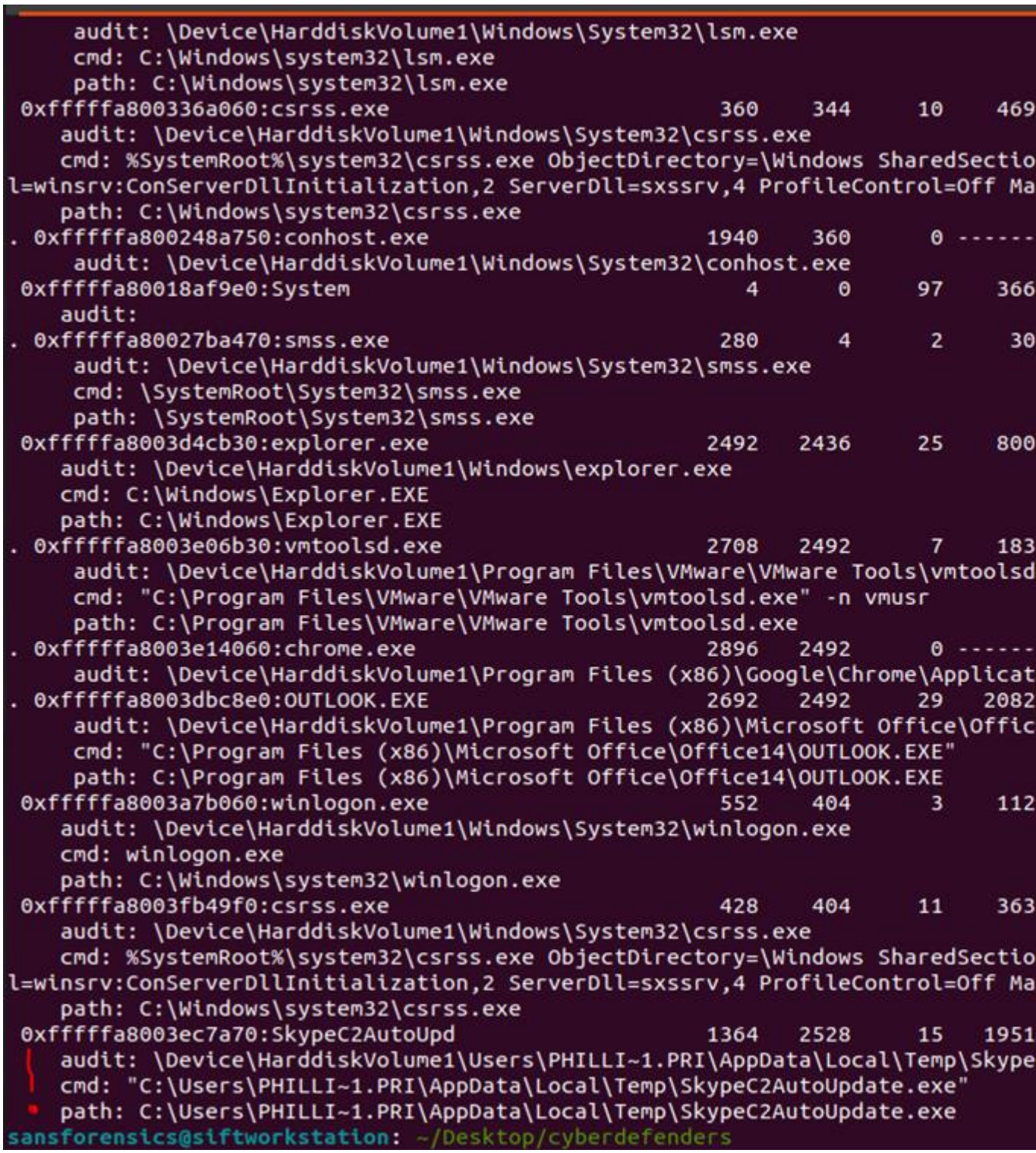


Рисунок 2 – Вывод pstree -v.

Можно заметить две интересных особенности для процесса SkypeC2AutoUpdate.exe (PID 1364):

1. **Путь из которого он был запущен** (часто вредоносы запускаются из пользовательской директории **%TEMP %**).
2. **Отсутствие информации о родительском процессе 2528**.

Гугл сказал, что у Dr.WEB в анализе трояна, использовался процесс с наименованием SkypeC2AutoUpdate.exe. Но пока рано делать выводы. Соберём чуть больше информации об учетной записи из под которой запустили процесс(рисунок 3):

vol.py getsids -p 1364

Рисунок 3 – получение информации о SIDS пользователей, запустивших процесс.

На рисунке 3 мы видим, что процесс запущен из под пользователя **phillip.price**, который входит в доменную группу и запустил процесс после входа через консоль.

Не менее интересными будут и сетевые соединения. Чтобы их посмотреть, воспользуемся командой:

vol.py netscan

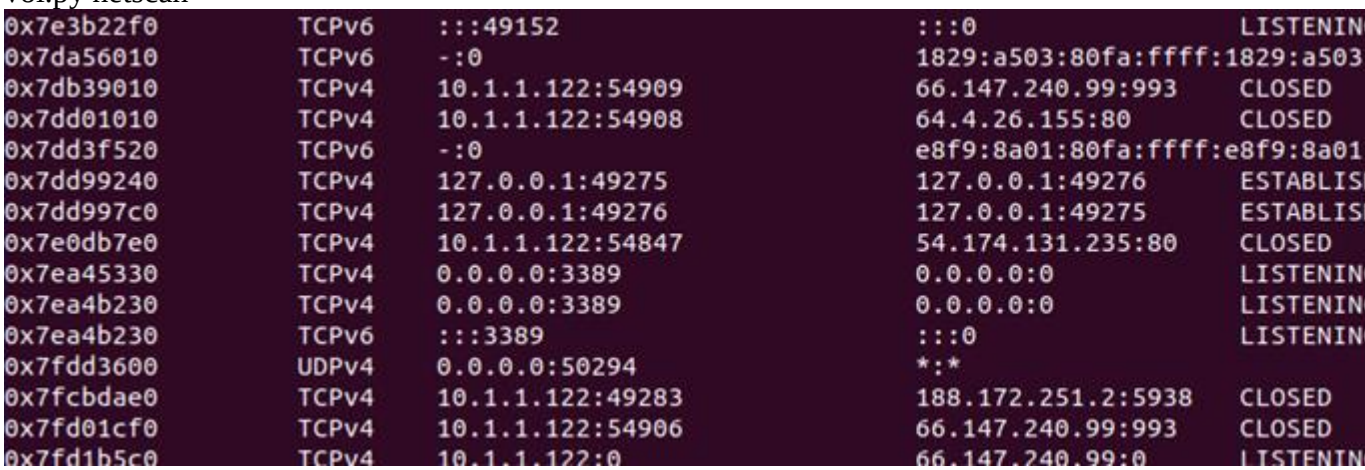


Рисунок 4 – соединения и процессы, породившие их.

Видно сторонние IPv4 и порты подключения, для процессов:

- SkypeC2AutoUpdate.exe: 54.174.131.235:80, 120.122.236.3;
- OUTLOOK.EXE: 66.147.240.99:993, 64.4.26.155:80.

В 5 вопросе задания нас просят указать e-mail отправителя фишингового письма (**What was the sender's email address that delivered the phishing email?**), найдём файлы с расширением ***.eml** или ***.pst** (такое расширение имеют файлы Outlook и Microsoft Exchange, могут содержать как сами письма, так и папки, контакты, адреса, вложения и.т.д).

В первом случае для *.eml файлов поиск результатов не дал, а вот во втором мы получаем несколько файлов с расширением pst.

Команда для поиска (результат на рисунке ниже):

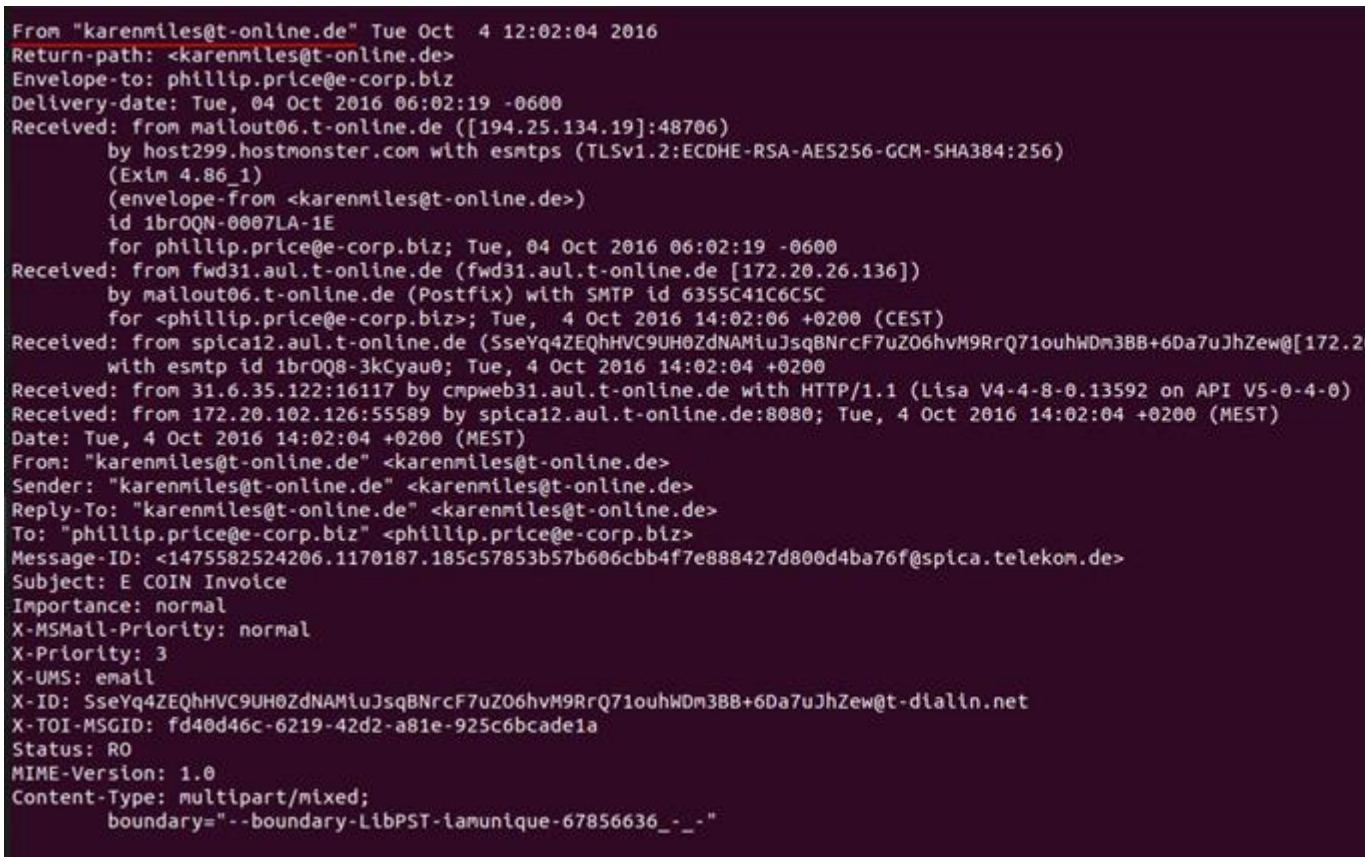
vol.py filescan | grep pst$

```
sansforensics@siftworkstation: ~/Desktop/GrrCon/ecorpoffice/pst2
$ vol.py filescan | grep pst$
Volatility Foundation Volatility Framework 2.6.1
0x000000007d4d0750     15      0 RW-r-- \Device\HarddiskVolume1\Users\phillip.price\Documents\Outlook Fil
0x000000007d4d9450     16      0 RW-r-- \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microso
0x000000007db2b520      8      8 RW-r-- \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microso
0x000000007fc9ee20     10      9 RW-r-- \Device\HarddiskVolume1\Users\phillip.price\Documents\Outlook Fil
0x000000007fd38c80      1      0 RW-r-- \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microso
sansforensics@siftworkstation: ~/Desktop/GrrCon/ecorpoffice/pst2
```

Сдампим файлы по имени, в специально созданную директорию pst2:
vol.py dumpfiles -n -i -r phillip.price@e-corp.biz.pst$ -D pst2
А теперь приступим к анализу файлов. Для этого воспользуемся утилитой **readpst** с флагом **-S** (подробнее):
readpst -S file.2692.0xfffffa80042dcf10.phillip.price@e-corp.biz.pst.dat

```
sansforensics@siftworkstation: ~/Desktop/GrrCon/ecorpoff
$ readpst -S file.2692.0xfffffa80042dcf10.phillip.price@
Opening PST file and indexes...
Processing Folder "Inbox"
Processing Folder "Trash"
Processing Folder "Sent"
        "phillip.price@e-corp.biz" - 2 items done, 0 ite
        "Sent" - 4 items done, 0 items skipped.
        "Inbox" - 13 items done, 3 items skipped.
sansforensics@siftworkstation: ~/Desktop/GrrCon/ecorpoff
$ ls phillip.price@e-corp.biz/Inbox/
10  11  12  13  13-bank_statement_088452.doc  3  4  5  6
```

Как мы видим, во входящих было сохранено 13 элементов, среди которых письма и вложение, в нашем случае вложение из письма №**13**, поэтому начинается так: **13**-bank_statement_088452.doc. Давайте выведем на экран содержимое писем. (рисунок 7 и 8)



```
From "karenmiles@t-online.de" Tue Oct  4 12:02:04 2016
Return-path: <karenmiles@t-online.de>
Envelope-to: phillip.price@e-corp.biz
Delivery-date: Tue, 04 Oct 2016 06:02:19 -0600
Received: from mailout06.t-online.de ([194.25.134.19]:48706)
        by host299.hostmonster.com with esmtps (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256)
        (Exim 4.86_1)
        (envelope-from <karenmiles@t-online.de>)
        id 1brOQN-0007LA-1E
        for phillip.price@e-corp.biz; Tue, 04 Oct 2016 06:02:19 -0600
Received: from fwd31.aul.t-online.de (fwd31.aul.t-online.de [172.20.26.136])
        by mailout06.t-online.de (Postfix) with SMTP id 6355C41C6C5C
        for <phillip.price@e-corp.biz>; Tue,  4 Oct 2016 14:02:06 +0200 (CEST)
Received: from spica12.aul.t-online.de (SseYq4ZEQhHVC9UH0ZdNAMiuJsqBNrcF7uZO6hvM9RrQ71ouhWDm3BB+6Da7uJhZew@[172.2
        with esmtp id 1brOQ8-3kCyau0; Tue, 4 Oct 2016 14:02:04 +0200
Received: from 31.6.35.122:16117 by cmpweb31.aul.t-online.de with HTTP/1.1 (Lisa V4-4-8-0.13592 on API V5-0-4-0)
Received: from 172.20.102.126:55589 by spica12.aul.t-online.de:8080; Tue, 4 Oct 2016 14:02:04 +0200 (MEST)
Date: Tue, 4 Oct 2016 14:02:04 +0200 (MEST)
From: "karenmiles@t-online.de" <karenmiles@t-online.de>
Sender: "karenmiles@t-online.de" <karenmiles@t-online.de>
Reply-To: "karenmiles@t-online.de" <karenmiles@t-online.de>
To: "phillip.price@e-corp.biz" <phillip.price@e-corp.biz>
Message-ID: <1475582524206.1170187.185c57853b57b606cbb4f7e888427d800d4ba76f@spica.telekom.de>
Subject: E COIN Invoice
Importance: normal
X-MSMail-Priority: normal
X-Priority: 3
X-UMS: email
X-ID: SseYq4ZEQhHVC9UH0ZdNAMiuJsqBNrcF7uZO6hvM9RrQ71ouhWDm3BB+6Da7uJhZew@t-dialin.net
X-TOI-MSGID: fd40d46c-6219-42d2-a81e-925c6bcade1a
Status: RO
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="--boundary-LibPST-iamunique-67856636_-_-"
```

Рисунок 7 – отправитель письма с вложением.

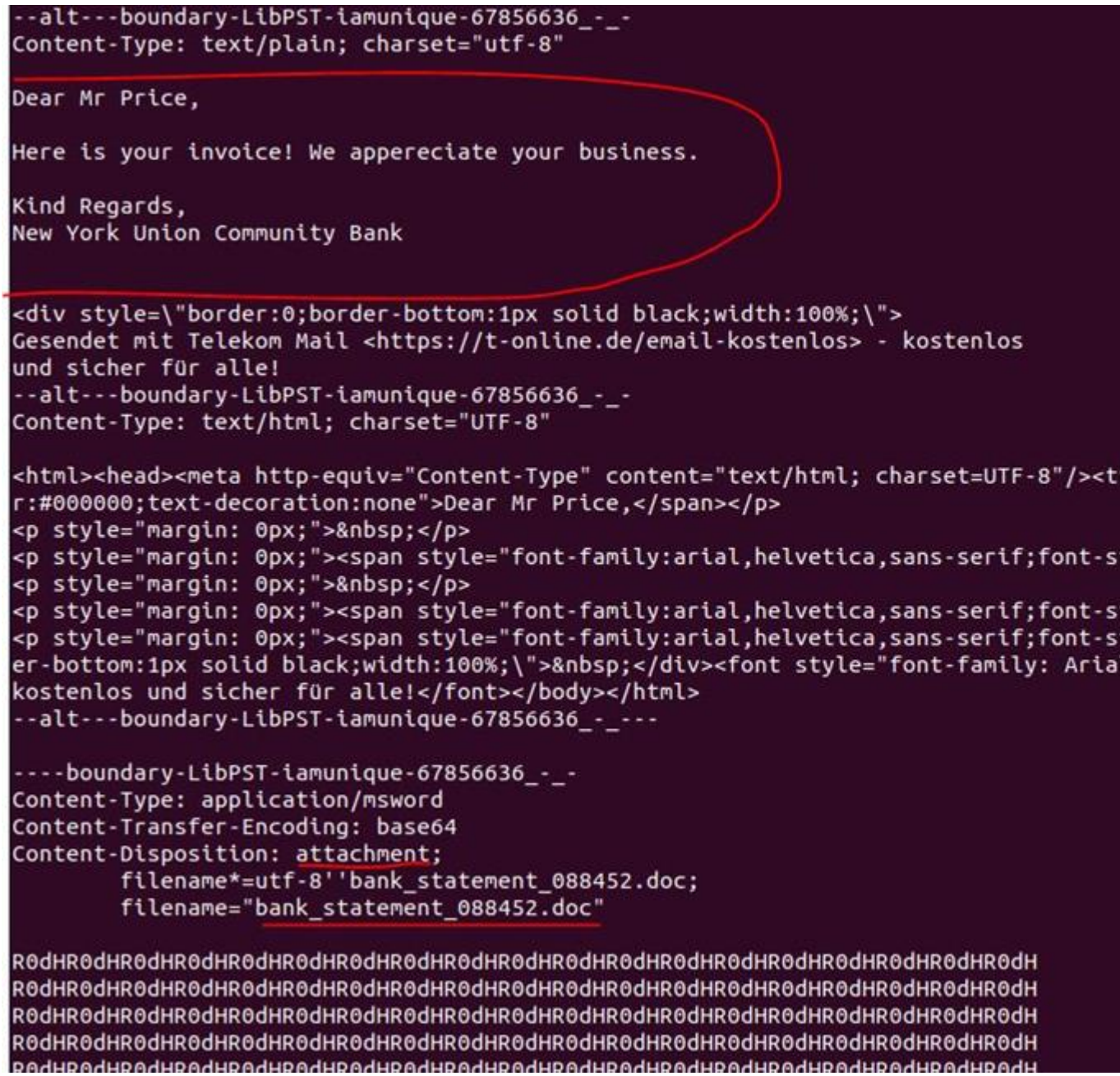


Рисунок 8 – текст и наличие вложения (attachment'a) с его названием.

3.1.4. Оценка освоения теоретического курса профессионального модуля по МДК.05.04

Дидактические единицы	**Проверяемые ОК, ПК, У, З**	**Формы контроля (наименование контрольной точки)**		
		Текущая аттестация		**Промежуточная аттестация**
Тема 51. Контрактная система в сфере закупок. Базовые принципы. Организация контрактной деятельно-	У10, З6, З7, ОК1-ОК11 ПК 1.6	Практическая работа № 9 Расчёт пени поставщику по 44-ФЗ	Устный зачет по теме 4.1	Теоретические вопросы на экзамене

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)		
		Текущая аттестация		Промежуточная аттестация
сти заказчика.				
Тема 4.2. Способы определения поставщика. Правила организации и проведения процедур определения поставщика. Конкурентные способы закупок. Закупка у единственного поставщика	У11, З6, З7, ОК1-ОК11 ПК 1.6	Практическая работа № 11 Решение задач. Алгоритм действий при признании аукциона несостоявшимся.	Устный зачет по теме 4.2	
Тема 4.3. Государственный (муниципальный) контракт. Приемка. Экспертиза. Контроль и ответственность заказчика	У12, З6, З7, ОК1-ОК11 ПК 1.7	Практическая работа № 20 Рассмотрение жалоб на действия (бездействие) закупающей организации	Устный зачет по теме 4.3	

1. Практическая работа № 9 Расчёт пени поставщику по 44-ФЗ

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

Условие: "Поставщик", по условиям контракта от 02.04.2018г. № 32, должен поставить "Заказчику": 3545 кг муки пшеничной 1 с. по цене 17 руб. 33 коп., 2560 кг муки пшеничной 2 с. по цене 13 руб. 42 коп., 3500 кг муки ржаной по цене 16 руб. 27 коп.

Контракт заключен по п. 5 ч. 1 ст. 93 Федерального закона от 5 апреля 2013г. № 44-ФЗ и действовал до 30.06.2018. Поставка осуществляется по заявкам "Заказчика" в течение 5

рабочих дней после получения заявки "Поставщиком". "Заказчик" направил заявку "Поставщику" на поставку 50 кг муки пшеничной 1с., 40 кг муки пшеничной 2с., 50 кг муки ржаной. Заявка получена "Поставщиком" 14.05.2018г. Доставка заявленной партии выполнена 05.06.2018г. Задание: необходимо по состоянию на 05.06.2018 года рассчитать пеню "Поставщику" за просрочку поставки партии товара в соответствии с Правилами, установленными постановлением Правительства РФ от 30.08.2017 N 1042, учитывая, что в остальной части товар был поставлен полностью в надлежащий срок.

Эталон ответа:

Постановлением Правительства РФ от 30.08.2017 N 1042 регламентирует определения размера штрафа, начисляемого в случае ненадлежащего исполнения заказчиком, неисполнения или ненадлежащего исполнения поставщиком (подрядчиком, исполнителем) обязательств, предусмотренных контрактом за исключением просрочки исполнения обязательств.

Определение пеней за просрочку регламентировано нормами ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" от 05.04.2013 N 44-ФЗ, в частности, статьей 34. Согласно п. 7 ст. 34 44-ФЗ пеня начисляется за каждый день просрочки исполнения поставщиком (подрядчиком, исполнителем) обязательства, предусмотренного контрактом, начиная со дня, следующего после дня истечения установленного контрактом срока исполнения обязательства, и устанавливается контрактом в размере одной трехсотой действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены контракта, уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных контрактом и фактически исполненных поставщиком (подрядчиком, исполнителем), за исключением случаев, если законодательством Российской Федерации установлен иной порядок начисления пени.

Актуальная ключевая ставка ЦБ РФ на период действия контракта: 7,25% годовых. Тогда К = 1/300*0,0725 = 0,000242 Период просрочки: с 22.05.18 по 05.06.2018 включительно, или 15 дней. Сумма просроченного к поставке товара: 50*17,33+40*13,42+50*16,27 = 2216,8 руб. или 2216 руб. 80 коп.

Величина пени: П = 2216,8*0,000242*15 = 8,05 руб. или 8 руб. 05 коп. Таким образом, пеня составит 8 руб. 05 коп.

Устный зачет по теме 4.1

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 6 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Назовите ⇦⇨➔🡽🡼➔⇦🞩 🡾⇩🡻⇨🞩⇩🡾⇧⇩➔ ➔ ⇦⇨🡾🡸⇨→🡽🡽🡾⇧⇩➔?
2. Назовите ⇦⇨➔🡽🡼➔⇦ 🡾↑🡼⇧⇦🡼🡽🡼🡽➔🖩 🡻🡾🡽🡻⇳⇨🡼🡽🡼➔➔?
3. Назовите ⇦⇨➔🡽🡼➔⇦ ⇦⇨🡾⇳🡼⇧⇧➔🡾🡽➔🡼➔🡸🡼→ 🡸→🡻→🡸🡽➔🡻→?
4. Назовите ⇦⇨➔🡽🡼➔⇦ ⇧⇩➔🡼⇳🡼➔🡾🡻→🡽➔🖩 ➔🡽🡽🡾🡻→🡼➔🡹?

5. Назовите критерии ↓×⇧↘🡻↘⇩↙↖↙↘↖↘↖➔⬀↙↘🡅 ⇦⇨↘↗⇔🡻⬀➔➔🖃 по которым их можно отнести к товарам, работам и услугам?
6. Назовите ⇦⇨➔↙⬀➔⇦ ↘⇩↓↙⇩⇧⇩↓↙↙↙↘⇧⇩➔ 🡐→ ⇨↙🡐⇔↖✓⇩→⇩➔↓↙↘⇧⇩✓ ↘🡅↙⇧⇦↙⬀↙↙➔🖷 ↖↘⇧⇔↗→⇨⇧⇩↓↙↙↙×↖ ➔ ↗⇔↙➔⬀➔⇦→↖✓↙×↖ ↙⇔↘↗🖃 🗷⇳⇳↙🡻⇩➔↓↙↘⇧⇩✓ ↘⇧⇔▫↙⇧⇩↓ ↖↙↙➔🖷 🡐→🡻⇔⇦↘🡻?

Эталоны ответов: приведены в учебном пособии по МДК.02.04 «Организация закупки оборудования и ПО».

2. Практическая работа № 11 Решение задач. Алгоритм действий при признании аукциона несостоявшимся

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

1. Опишите причины и возможные действия в случае признания аукциона несостоявшимся
2. Составьте таблицу действий.

Эталон ответа:

Действия заказчика в случае признания электронного аукциона несостоявшимся

Таблица 1

Этап, на котором закупка признается несостоявшейся	Причина признания закупки несостоявшейся	Действия заказчика
Подача заявок	Не подано ни одной заявки (ч.16 ст.66 Закона № 44-ФЗ)	Внесение изменений в план-график (при необходимости) и проведение запроса предложений в электронной форме или новой закупки (ч.4 ст.71 Закона № 44-ФЗ)
	Подана только одна заявка (ч.16 ст.66 Закона № 44-ФЗ)	Если заявка признана соответствующей требованиям – заключение контракта с единственным участником в соответствии с п.25 ч.1 ст.93 Закона № 44-ФЗ* (п.4 ч.1 ст.71 Закона № 44-ФЗ)
		Если заявка признана несоответствующей требованиям – внесение изменений в план-график (при необходимости) и проведение запроса предложений в электронной форме или новой закупки (ч.4 ст.71 Закона № 44-ФЗ)

Этап, на котором закупка признается несостоявшейся	Причина признания закупки несостоявшейся	Действия заказчика
Рассмотрение первых частей заявок	Принято решение об отказе в допуске к участию всех участников, подавших заявки (ч.8 ст.67 Закона № 44-ФЗ)	Внесение изменений в план-график (при необходимости) и проведение запроса предложений в электронной форме или новой закупки (ч.4 ст.71 Закона № 44-ФЗ)
	Принято решение о признании только одного участника, подавшего заявку, участником закупки (ч.8 ст.67 Закона № 44-ФЗ)	Рассмотрение второй части заявки. Если заявка признана соответствующей требованиям – заключение контракта с единственным участником в соответствии с п.25 ч.1 ст.93 Закона № 44-ФЗ* (п.4 ч.2 ст.71 Закона № 44-ФЗ)
		Рассмотрение второй части заявки. Если заявка признана несоответствующей требованиям – внесение изменений в план-график (при необходимости) и проведение запроса предложений в электронной форме или новой закупки (ч.4 ст.71 Закона № 44-ФЗ)
Подача предложений о цене контракта	В течение десяти минут после начала аукциона ни один из его участников не подал предложение о цене контракта (ч.20 ст.68 Закона № 44-ФЗ)	Заключение контракта в соответствии с п. 25 ч.1 ст.93 Закона № 44-ФЗ* с участником, заявка которого подана ранее других, при условии её соответствия требованиям (п.4 ч.3 ст.71 Закона № 44-ФЗ);
		Заключение контракта в соответствии с п. 25 ч.1 ст.93 Закона № 44-ФЗ* с единственным участником, если только один участник признан соответствующим требованиям (п.4 ч.3 ст.71 Закона № 44-ФЗ);
		Если все заявки признаны несоответствующими требованиям – внесение изменений в план-график (при необходимости) и проведение запроса предложений в электронной форме или новой закупки (ч.4 ст.71 Закона № 44-ФЗ)
Рассмотрение вторых частей заявок	Принято решение о несоответствии требованиям всех вторых частей заявок (ч.13 ст.69 Закона № 44-ФЗ)	Внесение изменений в план-график (при необходимости) и проведение запроса предложений в электронной форме или новой закупки (ч.4 ст.71 Закона № 44-ФЗ)
	Принято решение о соответствии требованиям только одной второй части заявки (ч.13 ст.69 Закона № 44-ФЗ)	Заключение контракта с единственным участником в соответствии с п.25 ч.1 ст.93 Закона № 44-ФЗ* (ч.3.1 ст.71 Закона № 44-ФЗ)

Этап, на котором закупка признается несостоявшейся	Причина признания закупки несостоявшейся	Действия заказчика
Заключение контракта	Уклонение или отказ победителя от заключения контракта в соответствии с ч. 13 ст. 83.2 Закона № 44-ФЗ (неподписание проекта контракта или ненаправление протокола разногласий)	Заключение контракта с участником процедуры, заявке которого присвоен второй номер (ч. 14 ст. 83.2 Закона № 44ФЗ)
	Уклонение или отказ победителя (участника процедуры, заявке которого присвоен второй номер) от заключения контракта в	Внесение изменений в план-график (при необходимости) и осуществление новой закупки либо осуществление закупки у единственного поставщика (подрядчика, исполнителя) в соответствии с п. 25 ч. 1 ст. 93 Закона № 44-ФЗ* (ч. 4 ст. 71

Устный зачет по теме 4.2

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 6 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Назовите условие об ответственности заказчика и поставщика за неисполнение или ненадлежащее исполнение обязательств по контракту (ч. 4 ст. 34 № 44-ФЗ)
2. Назовите условие о порядке и сроках оплаты ТРУ (ч. 13 ст. 34 № 44-ФЗ) – форма оплаты, аванс, срок и порядок оплаты
3. Назовите условие о порядке и сроках приемки поставленного товара, выполненной работы (ее результатов) или оказанной услуги (ч. 13 ст. 34)
4. Назовите условие о форме необходимого подтверждающего документа и дополнительных документах
5. Назовите условие о предоставлении обеспечения исполнения контракта (способ, сумма, срок обеспечения, реквизиты документов, подтверждающих его внесение) (ч. 1 ст. 96) и о его возврате
6. Назовите условие об одностороннем расторжении, если заказчик предусматривает такую возможность (ч.9 ст.95)

Эталоны ответов: приведены в учебном пособии по МДК.02.04 «Организация закупки оборудования и ПО».

3. Практическая работа № 20 Рассмотрение жалоб на действия (бездействие) закупающей организации

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

Ответьте на следующие вопросы:

1. Основания для обжалования решений закупающей организации
2. Кто вправе обжаловать действия /бездействие/ закупающей организации?
3. Куда подается жалоба на действия закупающей организации?
4. Как составить жалобу на закупающую организацию?
5. Рассмотрение жалобы на действия (бездействие) закупающей организации
6. Как рассматривается жалоба?

Эталон ответа:

Общая информация о подаче жалобы в ФАС по 44-ФЗ

Глава 6 ФЗ от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» устанавливает порядок обжалования действий организатора торгов, уполномоченного органа, учреждения, специализированной организации, комиссии по проведению торгов, должностного лица контрактной службы, контрактного управляющего, оператора ЭТП. Далее для краткости мы будем называть данный документ Законом о контрактной системе.

Практика показывает, что иногда заказчик игнорирует нормы Закона во время торгов. Тогда все их участники и лица, отвечающие за проверку общественных объединений, объединений юридических лиц, могут направить заявление в суд либо орган, занимающийся контролем проведения тендеров. Это делается для того, чтобы защититься от любых неправомочных поступков, которые мешают соблюдению прав, законных интересов потенциального исполнителя.

По закону возможна одновременная подача жалобы в контрольный орган в сфере закупок и в суд.

Порядок рассмотрения жалоб в ФАС устанавливается не только статьей 105 закона № 44-ФЗ, но и административным регламентом ФАС №727/14 от 19.11.2014 г.

Контрольные органы, которые уполномочены рассматривать жалобы по Закону № 44

Федеральным законом № 44 (часть 17, статья 105) определены контрольные органы в области закупок, уполномоченные на рассмотрение жалоб, и сказано, куда их следует направлять. На действия заказчиков подаются жалобы:

- в ФАС (Федеральную антимонопольную службу) в отношении тех закупок, которые обеспечивают федеральные и муниципальные нужды, а также нужды субъектов РФ;
- в органы исполнительной власти субъектов РФ, которые уполномочены осуществлять контроль в сфере госзакупок в отношении тех закупок, которые обеспечивают нужды субъектов РФ, а также нужды муниципальных образований;

- в органы местного самоуправления, уполномоченные осуществлять контроль в сфере госзакупок в отношении тех закупок, которые обеспечивают муниципальные нужды;

- жалобы на действия операторов ЭТП, подаваемые в Центральный аппарат Антимонопольной службы.

Кто имеет право подавать жалобу в ФАС по 44-ФЗ

ФАС отвечает за вопросы:

- по содержанию документации и правомерности установленных в ней требований;

- касающиеся действий/бездействий комиссии;

- относящиеся к действиям оператора ЭТП, в том числе имеющим отношение к получению аккредитации.

В первом случае обращение может исходить от любого юридического или физического лица, даже если оно не участвует в тендере. Вторая и третья ситуация распространяются только непосредственно на участников торгов, пострадавших от действий организаторов. Например, заявки отклонили без законных оснований на это, претенденты были лишены возможности подать ценовые предложение во время аукциона из-за сбоев в работе ЭТП, пр.

Перед тем как направить жалобу в ФАС по 44-ФЗ, вы должны понять, что именно вы собираетесь обжаловать. То есть выбрать определенные действия заказчика, пункт документации.

Когда у вас сложилось четкое представление, обратитесь к практике по данному вопросу – всю необходимую информацию вы найдете на сайте www.zakupki.gov.ru.

Всегда есть вероятность, что антимонопольная служба неоднократно рассматривала аналогичные проблемы по 44-ФЗ, вынося решение в пользу организатора тендера. Если вы нашли подтверждение этому, ваши шансы на победу будут очень низкими. Поэтому стоит подумать, нужно ли тратить время на подачу такого обращения.

Когда вы ознакомились со всеми доступными сведениями и сохранили уверенность, что ваши права нарушили, переходите к подготовке жалобы в ФАС по 44-ФЗ. На данном этапе важно выполнить требования по составлению данного документа, иначе бумагу могут вернуть.

Сроки подачи и виды жалоб в ФАС по 44-ФЗ

По 44-ФЗ для подачи разных видов жалоб в ФАС установлены такие сроки:

- на документы по аукциону – до завершения приема заявок на участие в закупках;

- на действия организатора – до 10 дней с момента публикации результатов торгов;

- если закон был нарушен в процессе рассмотрения вторых частей заявок/подписания контракта – до подписания госконтракта;

- на действия, имеющие отношение к заключению договора с победителем тендера – не позднее подписания госконтракта;

- на оператора ЭТП – 30 календарных дней со дня незаконных, по мнению участника, действий.

В первую группу входят обращения, связанные с несоблюдением норм закона положениями документации по закупке. Так, это может быть дополнение требований или перечня документов пунктами, не предусмотренными 44-ФЗ. Либо сюда относится отсутствие в тексте госконтракта конкретных сроков перечисления средств за выполнение работ, пр.

Под вторым видом обычно понимают обращения в ФАС по 44-ФЗ, связанные с неправомерными действиями во время распечатывания конвертов с заявками, котировочных заявок. А также жалобы могут иметь отношение к итогам тендера, когда победителем становится лицо, чья заявка не должна быть принята, согласно нормам закупочной документации. Либо речь может идти об отказе от допуска к торгам, признание заявки, не отвечающей уставленным нормам. Нужно понимать, что перечисленные виды можно включить и в третью группу обращений.

В четвертой группе встречаются жалобы на отказ от рассмотрения протокола разногласий к договору, от подписания соглашения по причинам, не имеющим под собой оснований, пр.

Реестр жалоб по Закону № 44

Федеральным законом № 44 предусмотрена необходимость включать в реестр жалоб следующую информацию: о подаваемых в контролирующие органы жалобах и принятых по итогам их рассмотрения решениях, о внеплановых и плановых проверках и принятых по их итогам решениях, а также о выданных предписаниях.

Размещаться реестр жалоб будет в ЕИС. Порядок ведения реестра, который включает, в частности, список размещаемой информации и сроки её размещения, будет утверждаться Правительством России.

Контрольный орган в области закупок в течение 2 дней (рабочих) с той даты, когда поступила жалоба, обязан разместить в информационной системе информацию, касающуюся поступления жалобы, а также её содержание, а затем направить заинтересованным лицам соответствующие уведомления. Информацию о решении, которое было вынесено в отношении жалобы, необходимо в течение 3 дней направить заинтересованным лицам и разместить на ЕИС в реестре жалоб.

Подготовка жалобы в ФАС по 44-ФЗ

Часть 8 ст. 105 44-ФЗ устанавливает, какая информация должна быть в обращении в ФАС. Это сведения:

- об организации, чьи действия считаются незаконными – название, контактные данные;
- об организации/физическом лице, подающем обращение по 44-ФЗ, – наименование, контактные данные;
- о закупке: реестровый номер на сайте www.zakupki.dov.ru либо информация об ЭТП, если закон нарушен в вопросах, имеющих отношение к получению аккредитации;
- о действиях/бездействиях, подлежащих обжалованию, – необходимо подробно перечислить пункты, реквизиты протокола и прочие нюансы в зависимости от вопроса.

Не стоит забывать, что обращение в ФАС по 44-ФЗ должно содержать информацию только по одним торгам. Если вам необходимо обжаловать действия заказчиков в нескольких торгах, документы подготавливаются отдельно для каждого случая нарушений.

Под жалобой должна стоять подпись уполномоченного лица, также необходимо прикрепить в качестве приложения бумаги, подтверждающие его права. Роль таких документов могут играть устав организации и приказ о назначении директора/генерального директора.

В процессе доказательства своей правоты участник тендера имеет право ссылаться как на положения 44-ФЗ, так и на другие документы. При этом необходимо указывать полные данные.

Как правильно подать жалобу в ФАС по 44-ФЗ: пошаговая инструкция

Если кратко, то, чтобы обратиться в антимонопольную службу, нужно:

- выбрать основания для обжалования;
- собрать доказательства нарушения норм закона;
- подготовить обращение;
- передать бумаги в ФАС.

Шаг 1. Определите основания для обжалования.

В первую очередь вам нужно понять:

- какие ваши права нарушены в процессе торгов;
- какие действия заказчика или оператора площадки были неправомерными;
- не завершился ли срок, установленный для обжалования подобных действий.

Основания и сроки подачи обращений, имеющих отношения к незаконным действиям организатора тендера, можно уточнить в ч. 4 ст. 105 44-ФЗ. Если вы считаете, что ваши права были нарушены оператором ЭТП, изучите положения ч. 5 ст. 105 44-ФЗ.

Шаг 2. Соберите доказательную базу.

Во время подготовки жалобы в ФАС по 44-ФЗ, помните, что в обращении необходимо подробно описать действия или решения госзаказчика/оператора, которые не являются законными. Все выводы необходимо подкрепить документами. В качестве аргументов может использоваться информация из:

- закона о контрактной системе, Закона 135-ФЗ и других ФЗ;
- подзаконных актов: постановлений правительства, приказов, распоряжений;
- разъяснительных писем Минфина, Минэкономразвития, ФАС;
- судебной практики: решений и постановлений;
- опубликованных решений УФАС – особенно убедительными для комиссии оказываются решения, вынесенные их коллегами в том же УФАС.

В каких случаях можно пожаловаться в ФАС на заказчика?

Спорные ситуации между заказчиком и участником закупок могут быть разнообразными.

Например, подать жалобу в ФАС по 44-ФЗ возможно в следующих случаях:

- нарушены положения закона о госзакупках в отношении обеспечения контракта – заказчик может выдвигать необоснованные требования к виду обеспечения;
- заказчик незаконно отказал компании или предпринимателю в допуске к торгам или препятствует исполнению контракта;
- заказчик «искусственно» ограничил количество участников закупки путем формирования требований, отраженных в закупочной документации;

- в документацию о закупке включены положения, согласно которым участники должны предоставить сведения или документы, предоставление которых не является обязательным в силу закона.

Это далеко не полный список тех нарушений, которые могут быть допущены заказчиком и обжалованы в ФАС. Понять, как действовать в той или иной спорной ситуации с заказчиком, поможет профессиональный юрист по 44-ФЗ. Обращение к юридическому специалисту по госзакупкам нашей компании поможет вам добиться справедливости и отстоять честное имя своей компании.

Закон позволяет обжаловать любому участнику закупки действия/бездействия не только самого заказчика, но и следующих лиц:

- специализированной организации;
- комиссии по осуществлению закупок;
- членов комиссии по осуществлению закупок;
- должностных лиц контрактной службы;
- контрактного управляющего;
- оператора электронной площадки.

Каковы сроки рассмотрения жалобы в ФАС по 44-ФЗ

Обращение, поданное в федеральную антимонопольную службу по 44-ФЗ, принимается либо отклоняется в течение двух рабочих дней с момента его поступления.

После этого заявитель и лицо, действия которого привели к составлению обращения по 44-ФЗ, получают уведомления о месте и времени проведения заседания. Также от них могут потребовать подать дополнительные документы, если проверяющие посчитают это нужным. Жалоба рассматривается максимум через 5 дней после ее принятия в присутствии сторон конфликта либо уполномоченных лиц. На заседании стороны могут приводить доводы, соглашаться или не соглашаться с мнением оппонента.

После заседания комиссии дается три рабочих дня, чтобы принять решение по вопросу. Далее последнее будет направлено представителям обеих сторон по электронной или обычной почте. Все решения ФАС по жалобам 44-ФЗ обжалуются только через арбитражный суд.

Срок подачи и рассмотрения

В п. 3-6 ст. 105 44-ФЗ перечислены сроки для передачи жалобы. Жалоба в отношении положения закупочной документации передается до окончания сроков подачи заявки. Жалоба на действия или бездействия заказчика передается в течение 10 дней после размещения в ЕИС протокола рассмотрения и оценки заявок на участие в конкурсе, запросе котировок и предложений или размещения на электронной площадке протоколов определения результатов аукциона.

Жалоба на действия или бездействие заказчика при рассмотрении второй части заявки на участие в аукционе подается до срока подписания контракта.

Когда указанные сроки истекли, жалоба передается в суд.

Антимонопольный орган вправе вернуть жалобу из-за несоответствия требованиям, согласно ч. 11 ст. 105 44-ФЗ, или рассмотреть ее. В ЕИС должно быть опубликовано уведомление о принятом ФАС решении. С его текстом необходимо ознакомить заказчика, поставщика и оператора.

Как минимум за 2 рабочих дня до даты рассмотрения спора участники должны направить в антимонопольную службу свои обоснования и возражения.

Основаниями для отказа в рассмотрении жалобы по существу могут являться:

1. **Отсутствие контактных сведений отправителя**, ФИО должного лица и адрес, по которому отправляется ответ.

2. **Жалоба содержит нецензурные и оскорбительные высказывания**.

3. **Текст обращения нечитабельный**.

4. **Обращение содержит вопрос, на который уже неоднократно передавались разъяснения**.

5. **В случае если для обращения требуется разглашение гостайны**.

6. **Текст обращения написан с использованием латиницы**.

7. **Жалоба была передана в электронном виде, но не подписана ЭЦП**.

После того как жалоба была зарегистрирована, у антимонопольной службы будет три рабочих дня на уведомление заявителя о месте и времени ее рассмотрения.

Антимонопольная служба будет рассматривать жалобу по существу в течение 5 рабочих дней. Решение инстанции подготавливается в письменном формате в течение 3 рабочих дней после оглашения резолюции и публикуется в ЕИС.

По результатам рассмотрения жалобы контролеры могут принять решение о ее признании необоснованной, частично обоснованной или полностью обоснованной. В последних двух случаях заказчику может быть выдано предписание об устранении нарушений, с которыми контролеры столкнулись в ходе разбирательств.

Если решение ФАС заявителя не удовлетворяет, то он вправе обжаловать его в арбитражном суде в течение 3 месяцев после принятия (на основании ч. 1, 4 ст. 198 АПК). На это участникам и заказчику отводится не более 3 месяцев.

В каких случаях могут отказать в рассмотрении жалобы в ФАС по 44-ФЗ

Обращение не рассматривается, если:

- в нем не выполняются установленные законом требования;
- под документами нет подписи либо стоит подпись лица, чьи полномочия не были подтверждены;
- истекло время, отведенное на подачу обращения;
- ФАС либо суд уже принял решение по указанным действиям.

Устный зачет по теме 4.3

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 6 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Назовите ⇦⇨➔🡽🡼➔⇦🞩 🡾⇩🡻⇨🞩⇩🡾⇧⇩➔ ➔ ⇦⇨🡾🡸⇨→🡼🡽🡾⇧⇩➔?
2. Назовите ⇦⇨➔🡽🡼➔⇦ 🡾↑🡼⇧⇦🡼🡼🡼🡽➔ 🡻🡾🡽🡻⇳⇨🡼🡽🡼➔➔?
3. Назовите ⇦⇨➔🡽🡼➔⇦ ⇦⇨🡾⇳🡼⇧⇧➔🡾🡽→🡭➔🡸🡽→ 🡸→🡻→🡸🡼➔🡻→?

4. Назовите ⇦⇨➔🡽🡕➔⇦ ⇧⇩➔🡕⇔🡼➔⇨🡾🡻➔🡽➔🖷 ➔🡽🡽🡾🡻➔🡕➔🡅?
5. Назовите критерии 🡻×⇧🡾🡻🡾⇩🡼🡖🡽🡾🡼🡾🡼➔🡔🡽🡾🡅 ⇦⇨🡾🡕⇔🡻🡕➔➔🖃 по которым их можно отнести к товарам, работам и услугам?
6. Назовите ⇦⇨➔🡽🡕➔⇦ 🡾⇩🡻🡼⇩⇧⇩🡻🡼🡽🡾⇧⇩➔ 🡐➔ ⇨🡼🡐⇔🡼✓⇩➔⇩➔🡻🡽🡾⇧⇩✓ 🡾🡅🡼⇧⇦🡼🡔🡼🡽➔🖷 🡖🡾⇧⇔🡕➔⇨⇧⇩🡻🡼🡽×🡖 ➔ 🡕⇔🡽➔🡕➔⇦➔🡼✓🡽×🡖 🡽⇔🡾🡕🖃 ☒⇳⇳🡼🡻⇩➔🡻🡽🡾⇧⇩✓ 🡾⇧⇔▫🡼⇧⇩🡻 🡼🡼🡽➔🖷 🡐➔🡻⇔⇦🡾🡻?

Эталоны ответов: приведены в учебном пособии по МДК.02.04 «Организация закупки оборудования и ПО».

3.1.5. Оценка освоения теоретического курса профессионального модуля по МДК.02.05

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 5.1. Основы управления проектами	ОК1-11 З8-З10 ПК1.7.	Устный зачет по Темам 1-2	Ответы на экзаменационные вопросы
Тема 5.2. Внутренняя и внешняя среда проекта	ОК1-11 З11 ПК1.7.		
Тема 5.3. Планирование проекта	ОК1-11 З12, З13, З14, З15 ПК1.7.	Устный зачет по Темам 3-4	
Тема 5.5. Управление проектными рисками	ОК1-11 З18 ПК1.7.		
Тема 5.5. Управление коммуникациями проекта	ОК1-11 З19, З12, З13, З14, З15 ПК1.7.	Устный зачет по Темам 5-8	
Тема 5.6. Информационные системы управления проектами			
Тема 5.7. Разработка и реализация проекта			
Тема 5.8. Управление качеством проекта и завершение проекта			

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 5.7. Разработка и реализация проекта	ОК1-11 У6, У7, У8 ПК1.7.	Практическая работа № 6. Презентация идеи проекта	
	ОК1-11 У9 ПК1.7.	Практическая работа № 18. Формирование диаграммы Ганта	
	ОК1-11 У10 ПК1.7.	Практическая работа № 25. Расчет плановых показателей эффективности реализации проекта	
	ОК1-11 ПК1.7. У6-У12	Практическая работа № 29. Презентация скорректированного проекта.	
	ОК1-11 У11 ПК1.7.	Практическая работа № 30. Расчет фактических показателей эффективности реализации проекта	
	ОК1-11 У6-12 ПК1.7.	Практическая работа № 31. Формирование отчета по проекту	
Тема 5.8. Управление качеством проекта и завершение проекта	ОК1-11 У6-У12 ПК1.7.	Практическая работа № 36. Презентация проекта	

1. Устный зачет по Темам 5.1-5.2

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Проектный менеджмент: понятие, характеристика, ключевые отличия проектного менеджмента от традиционного.
2. Проект как система. Системный подход к управлению проектами.

3. Цели проекта. Технология SMART постановки целей проекта. Требования, предъявляемые к проекту.
5. Окружение проекта. Участники проекта и их роли.
5. Жизненный цикл и структура проекта.

Эталоны ответов: приведены в Учебном пособии по МДК.02.05 «Управление проектами».

2. Устный зачет по Темам 5.3-5.4

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Основные задачи планирования проекта. Иерархическая структура работ проекта.
2. Распределение ресурсов. Разработка расписания проекта.
3. Анализ критического пути проекта: методы НИР, НОФ и МКР определения продолжительности проекта.
4. Оценка эффективности проекта: стоимость проекта, понятие и этапы оценки эффективности проекта, источники финансирования проекта.
5. Система управления проектными рисками. Основные подходы и методы управления рисками.

Эталоны ответов: приведены в Учебном пособии по МДК.02.05 «Управление проектами».

3. Устный зачет по Темам 5.5-5.8

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Управление коммуникациями проекта: роль и виды коммуникаций, планирование управления коммуникациями.
2. Информационные системы управления проектами: понятие, цели, задачи, функции.
3. Планирование и обеспечение качества проекта. Контроль качества проекта.

4. Основные процедуры закрытия проекта, составление окончательного отчета о реализации проекта.
5. Представление проекта заказчику, оценка проекта по его завершении.

Эталоны ответов: приведены в Учебном пособии по МДК.02.05 «Управление проектами».

5. Практическая работа № 6. Презентация идеи проекта

Инструкция для обучающихся
Внимательно прочитайте задание. Разработайте презентацию идеи проекта.

Время выполнения задания – 60 минут.

Задание 1. Создайте презентацию о вашем проекте.

В презентации должны быть отражены следующие аспекты:

1. Идея проекта и ее описание.
2. Команда проекта, распределение ролей.
3. Цели и задачи проекта.

Задание 2. Осуществите публичную защиту и презентацию вашего проекта, ответьте на вопросы преподавателя и группы, исправьте недочеты.

Задание 3. Вставьте скриншоты скорректированной презентации в отчет.

Эталон ответа:

ПРОЕКТ, НАЗНАЧЕНИЕ, КОМАНДА

Название: Оракул

Менеджер проекта: Авдонина Ю.А.

Команда проекта: Цховребадзе Р.Д., Авдонина Ю.А., Константинов В.В.

Характеристика продукта - обеспечение безопасности периметра организации.

Описание проблемы: угроза безопасности периметра организации. Незаконное проникновения на территорию.

Предлагаемая технология: установка систем наблюдения с распознаванием лица, с применением облачных технологий.

ЦЕЛИ И ЗАДАЧИ

Цели проекта:

- Обеспечить безопасности периметра организации путем внедрения и установки системы распознавания лиц
- Достичь максимального уровня стабильности соединения всех камер с облачным сервером.
- Внедрить систему Оракул в организацию с минимальными затратами для неё

Задачи проекта:

- Установка и настройка данной системы.
- Проверка системы на: исправную работу системы; корректный сбор информации; вывод информации с камер и передача ее в облачный сервер; сохранения информации на сервере; вывод информации для пользователей в реальном времени.
- Оптимизация системы.

ДОЛЖНОСТИ СОТРУДНИКОВ ПРОЕКТА

1. Куратор (Константинов) - Контроль исполнения проекта; Решение конфликтов, возникающих в проекте (ресурсные, межличностные и др.); Информирование Заказчика проекта о проблемах в проекте, находящихся в сфере его компетенции;

2. Ведущий разработчик(Цховребадзе) - написание кода; Делать код-ревью; Писать и рассматривать документацию по дизайну; Помогать коллегам, если они застряли; Поддерживать коллег на высоком уровне; Создавать новые проекты; Планировать работу своих проектов; Заранее сообщать о рисках проекта; Сообщать об успехах;

3. Руководитель проекта (Авдонина) – видение проекта как объекта управления, понимание его особенностей; анализ, учет интересов и управление отношениями со стейкхолдерами проекта; снижение неопределенности уникальной задачи за счет процедуры планирования; ресурсную базу проектных мероприятий и т.д.

ДОЛЖНОСТИ СОТРУДНИКОВ ПРОЕКТА

4. **Аккаунт (Авдонина)** - Осуществляет анализ аудитории потенциальных клиентов, выявляет потребности клиентов, их уровень и направленность; разрабатывает методики поиска клиентов, планирует работу с клиентами, составляет схемы обращения к клиентам; непосредственно осуществляет поиск клиентов всеми доступными способами (путем размещения рекламы, участия в выставках, ярмарках, презентациях, направления предложений по средствам коммуникаций, электронной почтой, факсимильными сообщениями, пр.); организует и проводит предварительные переговоры с клиентами, заинтересовавшимися предложениями (принявшими оферту, пр.), уточняет потребности каждого конкретного клиента и подготавливает предложение, адресованное определенному клиенту.

ДОЛЖНОСТИ СОТРУДНИКОВ ПРОЕКТА

5. Аналитик (Авдонина) – сбор сведений и их предварительная сортировка; анализ данных и их проверка; составление начальных предположений; создание точно регламентированных методических работ; формирование выводов и составление отчетности о проведенном исследовании.

6. Специалист по внедрению (Цховребадхе) - Осуществляет постановку задач по разработке и модификации офисного и корпоративного программного обеспечения в соответствии с изменением бизнес-процессов, процедур и целей компании; Планирует деятельность по решению этих задач и распределяет обязанности по их внедрению; Разрабатывает предложения по выбору нового программного обеспечения; Разрабатывает стандарты и методологии проектирования баз данных, разработки и внедрения программного обеспечения и т.д.

ПРОЦЕДУРА ОЦЕНКИ КОМАНДНЫХ РОЛЕЙ ПО Р. БЕЛБИНУ

Участники команды	Р	А	СВ	ВР	МР	А	К	Общее количество баллов
Цховребадзе			1	1				2
Авдонина	1	1				1		3
Константинов							1	1
Итого	1	1	1	1		1	1	6

ПОЛЬЗОВАТЕЛИ СИСТЕМЫ

- **Тип пользователя**: работники отдела безопасности; службы охраны (КПП):
- **Стандартный пользователь** (охранники, техники по безопасности) - использование данных с самих устройств, предоставляемые напрямую к пользователю
- **Вспомогательные пользователи** (сисадмин, специалист по безопасности) – помощь в настройке, помощь в использовании архива данных.
- Уровень технической грамотности:
  для стандартного специалиста – не требуется;
  для вспомогательных – высокий.
- Тех обслуживание камеры производится 1 раз в 2 недели; сбор информации с сервера производится раз в день, контроль за работой оборудования производится каждые полчаса.

ТРЕБОВАНИЯ К ПЛАТФОРМЕ И ПОТРЕБНОСТЯМ

1. Платформа для системы:

- Платоформа FindFace (облачный сервер объемов 8 ТБ)
- Камеры с разрешением Full HD (1080p)

2. Список потребностей для организации и пользователей:

Соблюдения режима безопасности входа и выхода в здание, определения лиц, нарушающих пропускной режим

КОМПОНЕНТЫ СИСТЕМЫ И ИХ ФУНКЦИИ

Облачный сервер – получает и хранит данные, полученные с камер.

Камеры – производит съемку и обработку данных, отправляет полученную информации на облачный сервер, потом передает стандартному пользователю.

КРАТКИЙ ОБЗОР ВОЗМОЖНОСТЕЙ

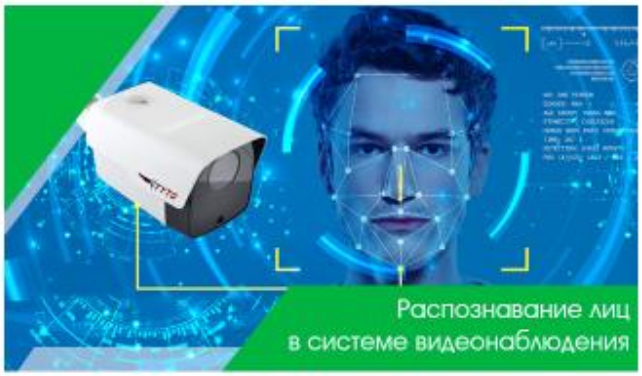
Предоставляемая возможность	Функция
Распознание лиц в реальном времени	Для определения лиц, нарушающих пропускного режима
Хранение данных о лицах, посещающих организацию	Для долгосрочного расследования инцидентов
Выполнение обработки информации самой камерой	Для быстрого получения информации в реальном времени

ФУНКЦИИ ПРОДУКТА

Функция	Статус	Приоритет	Риск	Стабильность
Определение лиц, нарушающих пропускного режима	Предложена	Критический	Средний	Средняя
Долгосрочное хранение информации с дальнейшим ее использованием.	Предложена	Важный	Низкий	Высокая
Возможность получения информации в реальном времени	Предложена	Критический	Средний	Высокая
Определение сотрудников организации из базы	Предложена	Полезная	Низкий	Высокая

РЕЗУЛЬТАТЫ ПРОЕКТА

Установка всего оборудования, используемого для системы видеонаблюдения, создание стабильной связи между всеми камерами и сервером, настройка оборудования организации для использования системы.



7. Практическая работа № 18. Формирование диаграммы Ганта

Инструкция для обучающихся
Внимательно прочитайте задание. Сформируйте диаграмму Ганта для своего проекта.

Время выполнения задания – 60 минут.

Задание 1. Установите длительность задач.

Для формирования диаграммы Ганта необходимо установить длительность задач.

Задание 2. Активизируйте вкладку «Сведения о задаче». На листе «Предшественники» выберите задачу-предшественника, установите тип связи и при необходимости запаздывание.

Вставьте скриншот

Задание 3. Сформируйте отчет в виде презентации проекта, в котором опишите в слайдах выбранные и назначенные трудовые и материальные ресурсы проекта, длительность выполнения операций (продолжительность реализации всего проекта), добавьте в презентацию скриншот графического отображения реализации проекта с назначенными ресурсами и длительностью (правая часть экрана в программе MS Project).

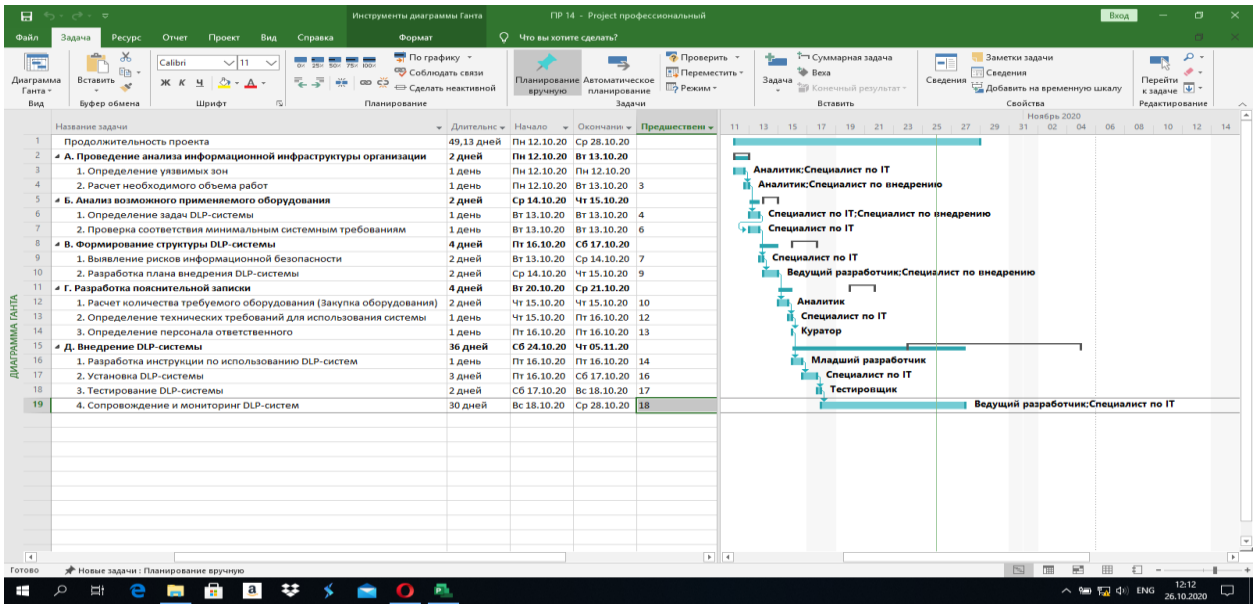
Вставьте скриншоты презентации в отчет

Эталон ответа:

Задание 1.

Связь между двумя задачами позволяет понять, каким образом время начала или завершения одной задачи влияет на время начала или завершения другой. Задача, влияющая на другую задачу, называется **Предшественник**, а задача, зависящая от другой, называется **Последователь**. Одна связь может объединять только две задачи, и при этом у одной задачи может быть несколько связей с другими задачами. Задача может иметь неограниченное число предшествующих и последующих задач. Связи могут объединять не только задачи, но и фазы, к которым применимы все принципы организации связей между задачами.

Задание 2.



Задание 3.

Трудовые ресурсы

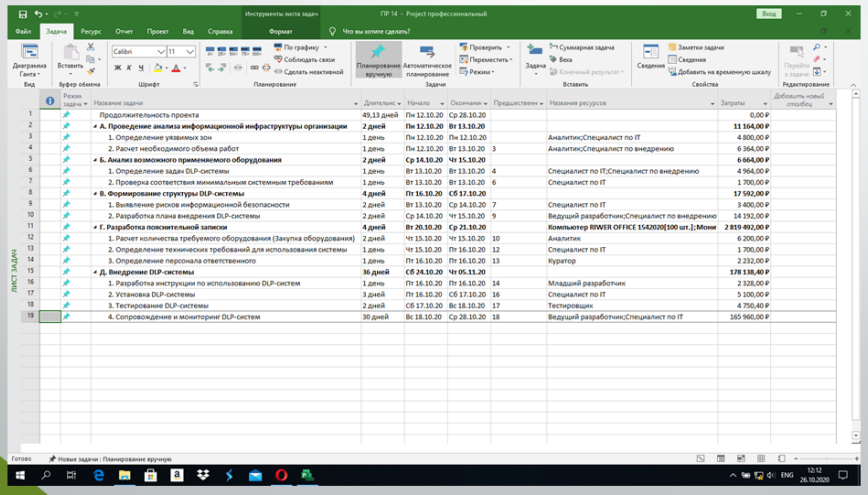
Трудовые ресурсы		
Наименование	Количество	Стоимость, руб.
Руководитель проекта	1	135 000
Аналитик	1	93 000
Ведущий разработчик	1	115 000
Младший разработчик	1	70 000
Специалист по внедрению	2	98 000
Куратор	1	67 000
Специалист по IT	1	51 000
Тестировщик	2	71 250
Итого	10	700 250

Материальные ресурсы

Материальные ресурсы		
Наименование	Количество	Стоимость
Компьютер RIWER OFFICE 1542020 https://www.ironbook.ru/catalog/computers/1542020/	100	19 428 р.
Монитор Samsung S22B300N https://www.ittelo.ru/partsittelo/monitory/Samsung-S22B300N	101	5 000 р.
Сервер HP Proliant DL360 Gen10 (P19178-B21) https://www.regard.ru/catalog/tovar334427.htm	1	361 560 р.
Итого	202	1 060 780р.

Продолжительность реализации всего проекта

Продолжительность реализации проекта определена в 36 дней.



7. Практическая работа № 25. Расчет плановых показателей эффективности реализации проекта

Инструкция для обучающихся

Внимательно прочитайте задание. Рассчитайте плановые показатели эффективности реализации проекта.

Время выполнения задания – 60 минут.

Задание 1. Определите внутреннюю норму рентабельности, норму прибыли, чистую текущую стоимость инвестиций, вложенных в реализацию проекта, используя исходные

данные, представленные в Приложении 1 (файл ПР 18. Приложение 1). Постройте график функции NPV этого проекта.

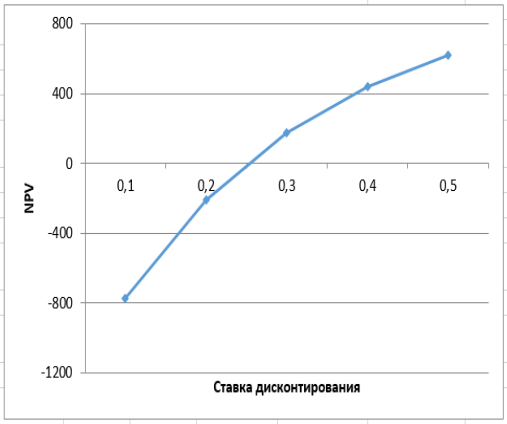
2	Инвестиционная компания рассматривает проект освоения внедрения новой компьютерной установки:					
3	предполагается вложить в производство			1600 тыс. руб.,		
4	получить в течение первого года			10000 тыс. руб. дохода, исчерпав ресурсы компании,		
5	и в течение второго года внедрить дополнительные ресурсы,					
6	вложив в это		10000 тыс. руб. Необходимо построить график функции NPV(Y) этого проекта.			
7	Безрисковая ставка равна		10%			
8	Период - год	0	1	2		
9	Оттоки (-E)					
10	Притоки (I)					
11	Денежный поток (CF)					
12	Внутренняя норма рентабельности (IRR)					
13	Норма прибыли (ARR)					
14	Зависимость NPV от норма отдачи (Y)					
15	Норма отдачи (Y)	10%	20%	30%	40%	50%
16	Чистая текущая стоимость (NPV)					
17						
18	Текущая стоимость оттоков PV(-E)					
19	Период	0	1	2		
20	Модифицированные денежные потоки для MIRR					
21	Модифицированная внутренняя норма рентабельности (MIRR)					

Вставьте скриншот решения

Эталон ответа:

Задание 1.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
2	Инвестиционная компания рассматривает проект внедрения новой компьютерной установки:													
3	предполагается вложить в производство		1600	тыс. руб.,										
4	получить в течение первого года		10000	тыс. руб. дохода, исчерпав ресурсы компании,										
5	и в течение второго года внедрить дополнительные ресурсы,													
6	вложив в это		10000	тыс. руб. Постройте график функции NPV(Y) этого проекта.										
7	Безрисковая ставка равна		10%											
8	Период - год	0	1	2										
9	Отток (-E)	-1600		-10000										
10	Притоки (I)		10000											
11	Денежный поток (CF)	-1600	10000	-10000										
12	Внутренняя норма рентабельности (IRR)	25%												
13	Норма прибыли (ARR)	-7%												
14	Зависимость NPV от норма отдачи (Y)													
15	Норма отдачи (Y)	10%	20%	30%	40%	50%								
16	Чистая текущая стоимость (NPV)	0,00р.	0,00р.	0,00р.	0,00р.	0,00р.								
17														
18	Текущая стоимость оттоков PV(-E)	-9 864,46р.												
19	Период	0	1	2										
20	Модифицированные денежные потоки для MIRR	-9 864,46р.	10 000,00р.	0,00р.										
21	Модифицированная внутренняя норма рентабельности (MIRR)	1%												
22														



8. Практическая работа № 29. Презентация скорректированного проекта

Инструкция для обучающихся

Внимательно прочитайте задание. Разработайте презентацию скорректированного проекта.

Время выполнения задания – 60 минут.

Задание 1. Создайте презентацию скорректированного проекта.

В презентации должны быть отражены следующие аспекты:

1. Идея проекта и ее описание.
2. Команда проекта, распределение ролей.
3. Цели и задачи проекта.
4. Описание произошедшей форс-мажорной ситуации.
5. Стадии проекта.
6. Продолжительность проекта по стадиям (скорректированная). Обоснование выбора оптимального метода продолжительности реализации проекта.
7. Трудовые и материальные ресурсы проекта (скорректированные).
8. Бюджет проекта (скорректированный).

Задание 2. Осуществите публичную защиту и презентацию вашего проекта, ответьте на вопросы преподавателя и группы, исправьте недочеты.

Задание 3. Вставьте скриншоты скорректированной презентации в отчет.

Эталон ответа:

ПРОЕКТ, НАЗНАЧЕНИЕ, КОМАНДА

Название: Оракул

Менеджер проекта: Авдонина Ю.А.

Команда проекта: Цховребадзе Р.Д., Авдонина Ю.А., Константинов В.В.

Характеристика продукта - обеспечение безопасности периметра организации.

Описание проблемы: угроза безопасности периметра организации. Незаконное проникновения на территорию.

Предлагаемая технология: установка систем наблюдения с распознаванием лица, с применением облачных технологий.

ЦЕЛИ И ЗАДАЧИ

Цели проекта:

- Обеспечить безопасности периметра организации путем внедрения и установки системы распознавания лиц
- Достичь максимального уровня стабильности соединения всех камер с облачным сервером.
- Внедрить систему Оракул в организацию с минимальными затратами для неё

Задачи проекта:

- Установка и настройка данной системы.
- Проверка системы на: исправную работу системы; корректный сбор информации; вывод информации с камер и передача ее в облачный сервер; сохранения информации на сервере; вывод информации для пользователей в реальном времени.
- Оптимизация системы.

СТАДИИ ПРОЕКТА

Были определены следующие стадии реализации проекта:

A. препроектные исследование

- Анализ плана местности
- Анализ плана этажа
- Изучить схему электропроводки здании

B. Техническое задание

- Разработка ТЗ
- Согласование ТЗ
- Утверждение ТЗ

C. Техническое предложение

- Проверка совместимости оборудования
- Выбор оптимального плана установки оборудования
- Обоснование установки
- Согласование предложения

D. Эскиз проекта

- Разработка эскиза
- Согласование эскиза
- Утверждение эскиза

E. Технические проект

- Разработка окончательного проекта системы
- Согласование проекта
- Утверждение проекта

F. Рабочий проекта

- Разработка рабочей документации

J. Монтаж системы

- Установка системы
- Первичная настройка системы

H.Тестирование системы

- Проверка системы при различных ситуациях
- Оптимизация системы
- Настройка системы после оптимизации

K. Эксплуатация

- Проведения ознакомления сотрудников с системой
- Проведение мероприятий для проверки знаний сотрудников по использованию системы

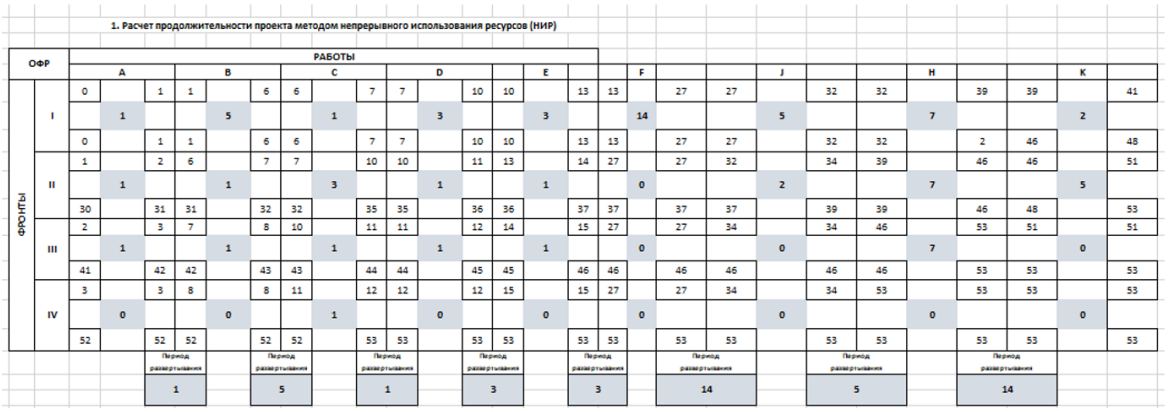
ПРОДОЛЖИТЕЛЬНОСТЬ РЕАЛИЗАЦИИ ВСЕГО ПРОЕКТА

Продолжительность реализации проекта определена в 53 дней

Задачи						
A. предпроектные исследование	**3 дней**	**Пн 02.11.20**	**Ср 04.11.20**			**20 048,00 ₽**
1. анализ плана местности	1 день	Пн 02.11.20	Пн 02.11.20		Аналитик;Охранники	5 016,00 ₽
2. анализ плана этажа	1 день	Вт 03.11.20	Вт 03.11.20		Аналитик;Охранники	5 016,00 ₽
3. изучить схему электропроводки в здании	1 день	Ср 04.11.20	Ср 04.11.20		Аналитик;Охранники;Специалист по безопасности;Техник по безопасности	10 016,00 ₽
B. Техническое задание	**7 дней**	**Вт 03.11.20**	**Ср 11.11.20**			**57 400,00 ₽**
1. разработка ТЗ	5 дней	Вт 03.11.20	Пн 09.11.20		Аналитик;Специалист по безопасности;Те	41 000,00 ₽
2. согласование ТЗ	1 день	Вт 10.11.20	Вт 10.11.20		Аналитик;Специалист по безопасности;Те	8 200,00 ₽
3. утверждение ТЗ	1 день	Вт 03.11.20	Вт 03.11.20		Аналитик;Специалист по безопасности;Те	8 200,00 ₽
C. Технические предложение	**6 дней**	**Вт 10.11.20**	**Вт 17.11.20**		**Камера HDcom FD116-S[10 шт];Монитор Samsung C49HG90DMI 48.9"[1 шт];Настольный компьютер Lenovo ThinkCentre M720q Tiny[1 шт];Платформа FindFace[1 шт]**	**765 920,00 ₽**
1. проверка совместимости оборудования	1 день	Вт 10.11.20	Вт 10.11.20		Сисадмин;Специалист по безопасности;Техник по безопасности	7 960,00 ₽
2. выбор оптимального плана установки оборудования	3 дней	Ср 11.11.20	Пт 13.11.20		Сисадмин;Специалист по безопасности;Техник по безопасности	23 880,00 ₽
3. обоснование установки	1 день	Ср 11.11.20	Ср 11.11.20		Сисадмин;Специалист по безопасности;Техник по безопасности	7 960,00 ₽
4. согласование предложения	1 день	Чт 12.11.20	Чт 12.11.20		Сисадмин;Специалист по безопасности;Техник по безопасности	7 960,00 ₽
D. Эскиз проекта	**5 дней**	**Ср 11.11.20**	**Вт 17.11.20**			**41 000,00 ₽**
1. разработка эскиза	3 дней	Ср 11.11.20	Пт 13.11.20		Аналитик;Специалист по безопасности;Те	24 600,00 ₽
2. согласование эскиза	1 день	Пн 16.11.20	Пн 16.11.20		Аналитик;Специалист по безопасности;Техник по безопасности	8 200,00 ₽
3. утверждение эскиза	1 день	Вт 17.11.20	Вт 17.11.20		Аналитик;Специалист по безопасности;Техник по безопасности	8 200,00 ₽
E. Технический проект	**5 дней**	**Пн 16.11.20**	**Пт 20.11.20**			**41 000,00 ₽**

ПРОДОЛЖИТЕЛЬНОСТЬ РЕАЛИЗАЦИИ ВСЕГО ПРОЕКТА

Продолжительность реализации проекта определена в 53 дней



1. Расчет продолжительности проекта методом непрерывного использования ресурсов (НИР)

ОФР		РАБОТЫ																													
		A			B			C			D			E			F			J			H			K					
ФРОНТЫ	I	0		1	1		6	6		7	7		10	10		13	13		27	27		32	32		39	39		41			
			1			5			1			3			3			14			5			7			2				
	II	0		1	1		6	6		7	7		10	10		13	13		27	27		32	32		2	46		48			
		1		2	6		7	7		10	10		11	13		14	27		27	32		34	39		46	46		51			
			1			1			3			1			1			0			2			7			5				
	III	30		31	31		32	32		35	35		36	36		37	37		37	37		39	39		46	48		53			
		2		3	7		8	10		11	11		12	14		15	27		27	34		34	46		53	51		51			
			1			1			1			1			1			0			0			7			0				
	IV	41		42	42		43	43		44	44		45	45		46	46		46	46		46	46		53	53		53			
		3		3	8		8	11		12	12		12	15		15	27		27	34		34	53		53	53		53			
			0			0			1			0			0			0			0			0			0				
		52		52	52		52	52		53	53		53	53		53	53		53	53		53	53		53	53		53			
				Период развертывания			Период развертывания			Период развертывания			Период развертывания			Период развертывания			Период развертывания			Период развертывания			Период развертывания						
				1			5			1			3			3			14			5			14						

9. Практическая работа № 30. Расчет фактических показателей эффективности реализации проекта

Инструкция для обучающихся

Внимательно прочитайте задание. Рассчитайте фактические показатели эффективности реализации проекта.

Время выполнения задания – 60 минут.

Задание 1. Определите внутреннюю норму рентабельности, норму прибыли, чистую текущую стоимость инвестиций, вложенных в реализацию вашего проекта, используя данные, полученные по результатам выполненных практических работ. Постройте график функции NPV вашего проекта.

Задание 2. Вставьте результаты расчета в виде скриншотов в отчет по практической работе.

Эталон ответа:

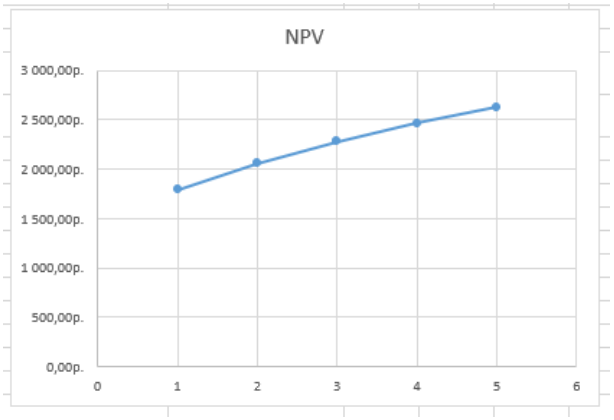
Задание 1.

Внутренняя норма рентабельности = 20%

Норма прибыли = 22%

Чистая текущая стоимость инвестиций = 5 000 000 руб.

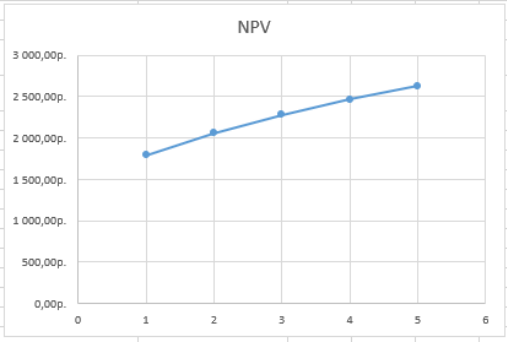
График функции NPV проекта:



Задание 2.

Инвестиционная компания рассматривает проект внедрения новой компьютерной установки:
предполагается вложить в производство 1600 тыс. руб.,
получить в течение первого года 10000 тыс. руб. дохода, исчерпав ресурсы компании,
и в течение второго года внедрить дополнительные ресурсы,
вложив в это 10000 тыс. руб. Необходимо построить график функции NPV(Y) этого проекта.

Безрисковая ставка равна		10%			
Период - год	Октябрь	Ноябрь	Декабрь		
Оттоки (-E)	-3202	-166	-160		
Притоки (I)			5000		
Денежный поток (CF)	-3202	-166	4 840,00р.		
Внутренняя норма рентабельности (IRR)	20%				
Норма прибыли (ARR)	22%				
Зависимость NPV от норма отдачи (Y)					
Норма отдачи (Y)	10%	20%	30%	40%	50%
Чистая текущая стоимость (NPV)	1 791,90р.	2 056,39р.	2 278,70р.	2 468,16р.	2 631,56р.
Текущая стоимость оттоков PV(-E)	798,00р.				
Период	0	1	2		
Модифицированные денежные потоки для MIRR	798,00р.	-166,00р.	-160,00р.		
Модифицированная внутренняя норма рентабельности (MIRR)	-44%				



10. Практическая работа № 26. Формирование отчета по проекту

Инструкция для обучающихся
Внимательно прочитайте задание. Сформируйте и оформите отчет по проекту.

Время выполнения задания – 60 минут.

Задание 1. Сформируйте отчет по проекту посредством экспорта и импорта проекта.

Экспорт и импорт данных позволяют работать с основными данными по проекту в других приложениях Microsoft, а также обеспечивают работу с XML файлами.
Для **экспорта** данных необходимо выполнить команду **Файл - Сохранить как** и выбрать тип файла **Книга Excel**.
Далее загружается **Мастер экспорта** файла, необходимо последовательно действовать по его указаниям.

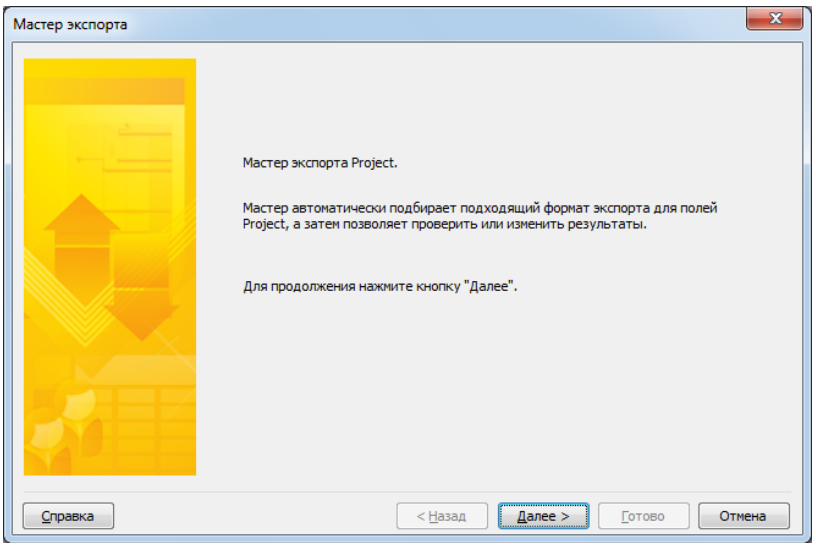


Рис. Мастер экспорта файла

- При необходимости экспорта всех данных проекта установить флажок **Шаблон проекта**. Если будут экспортироваться выборочные данные - установить флажок **Выбранные данные**.
- Установить флажок **Выбранные данные**, нажать **Далее**.
- На следующем шаге установить флажок **Создать новую схему**.
- В установках параметров схемы задать тип данных для экспорта - выбрать **Задачи** и **Назначения**, установить флажок **Включать заголовки при экспорте**.

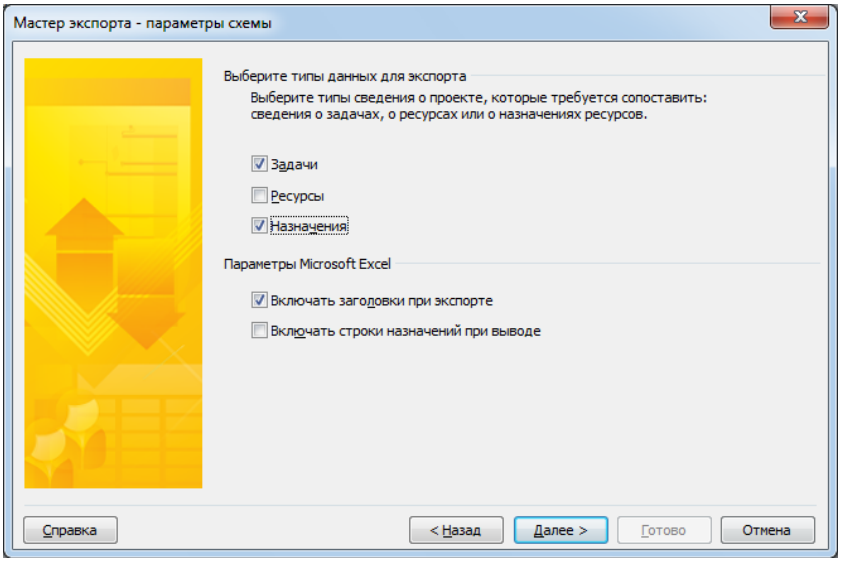


Рис. Мастер экспорта проекта - установка параметров

- Выполнить **настройку сопоставления данных** для таблицы Задач в соответствии с параметрами, отображенными в окне **Мастер экспорта**.
- Нажать кнопку **Далее** и выполнить **настройку сопоставления данных** для таблицы Назначений в соответствии с параметрами, отображенными в окне **Мастер экспорта.**

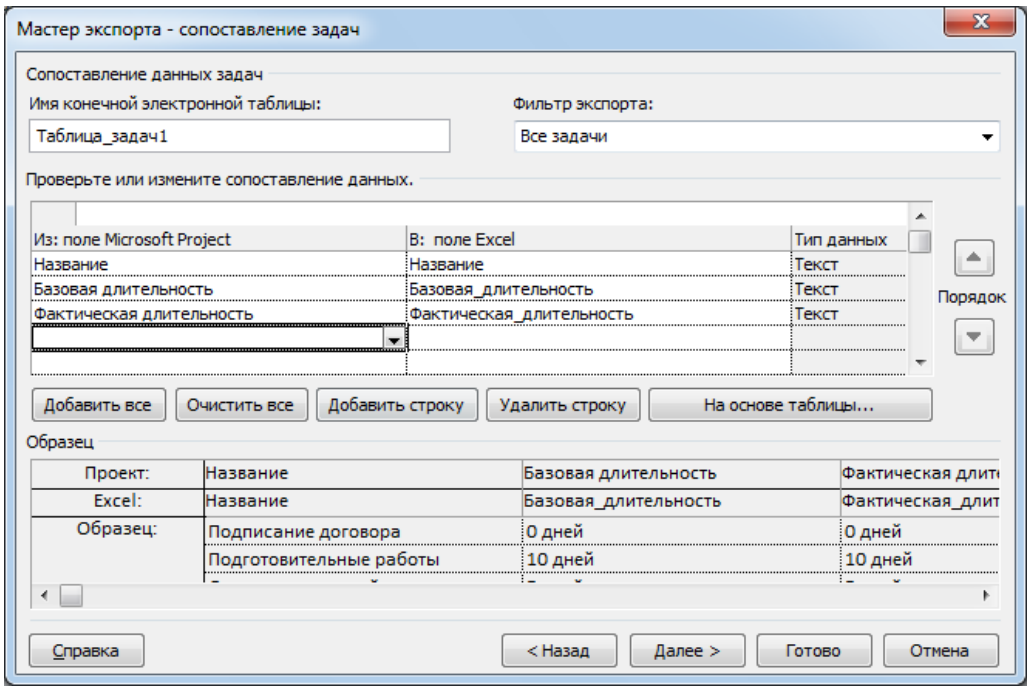


Рис. Мастер экспорта - Сопоставление задач

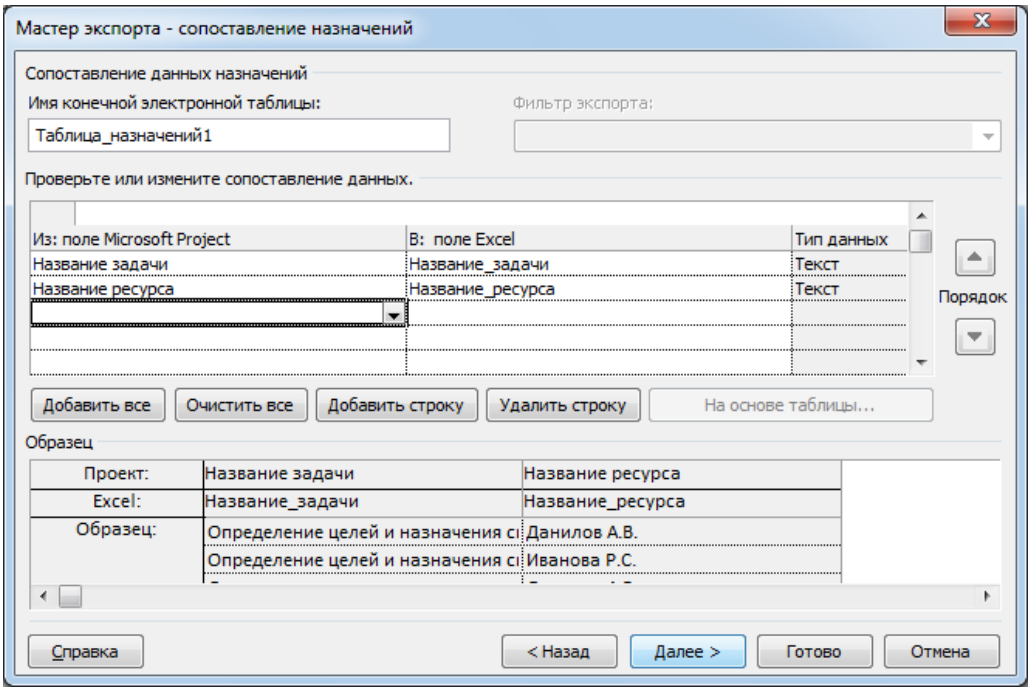


Рис. Мастер экспорта - Сопоставление назначений

- Затем, не сохраняя схему, нажать **Готово**.
- Открыть файл выгрузки данных и ознакомиться с результатом.

Импорт из MSExcel осуществляется путем открытия файла xls в MSProject.

- Выполнить команду **Файл - Открыть**. В появившейся форме выбрать тип файла **Книга Excel**.
- Выбрать экспортированный ранее файл.
- Далее производится пошаговая работа с **Мастером импорта**.
- Следующим шагом выбрать **Создать новую схему**. Нажать кнопку **Далее**.

- Установить флажок **Создать новый проект**, нажать кнопку **Далее**.
- Выбрать тип данных для импорта - так как ранее были экспортированы Задачи и Назначения, установить флажки **Задачи и Назначения**.
- Проверить на следующих шагах сопоставление данных - изменять ничего не следует, если указаны выбранные при экспорте параметры.

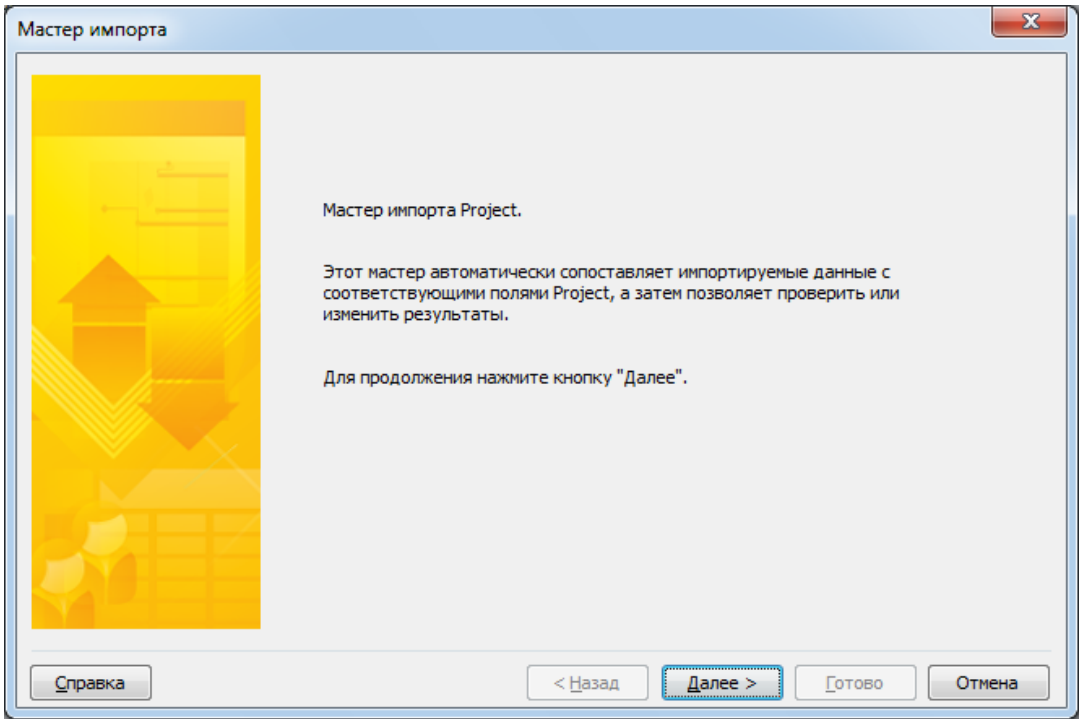


Рис. Мастер импорта проекта

- Завершить работу с **Мастером импорта**, нажать кнопку **Готово**.

Задание 2. В отчет по практической работе вставьте скриншоты выполненных операций. В СДО прикрепите отчет по практической работе (.docx), файл экспорта проекта (.xls), импортированный проект (.mpp).

Эталон ответа:

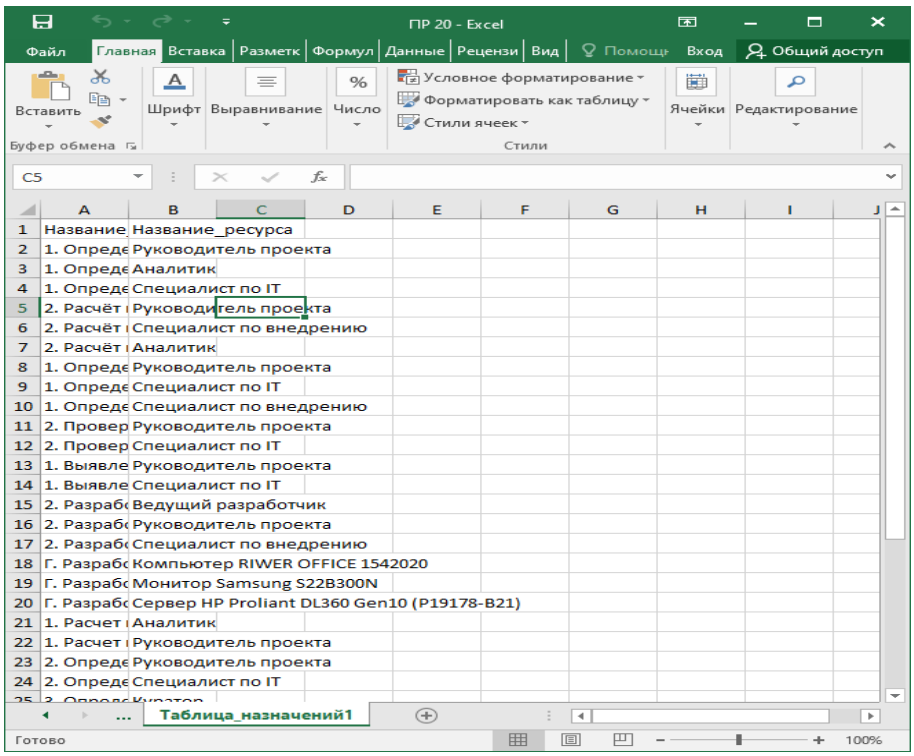


Рисунок – Таблица назначений

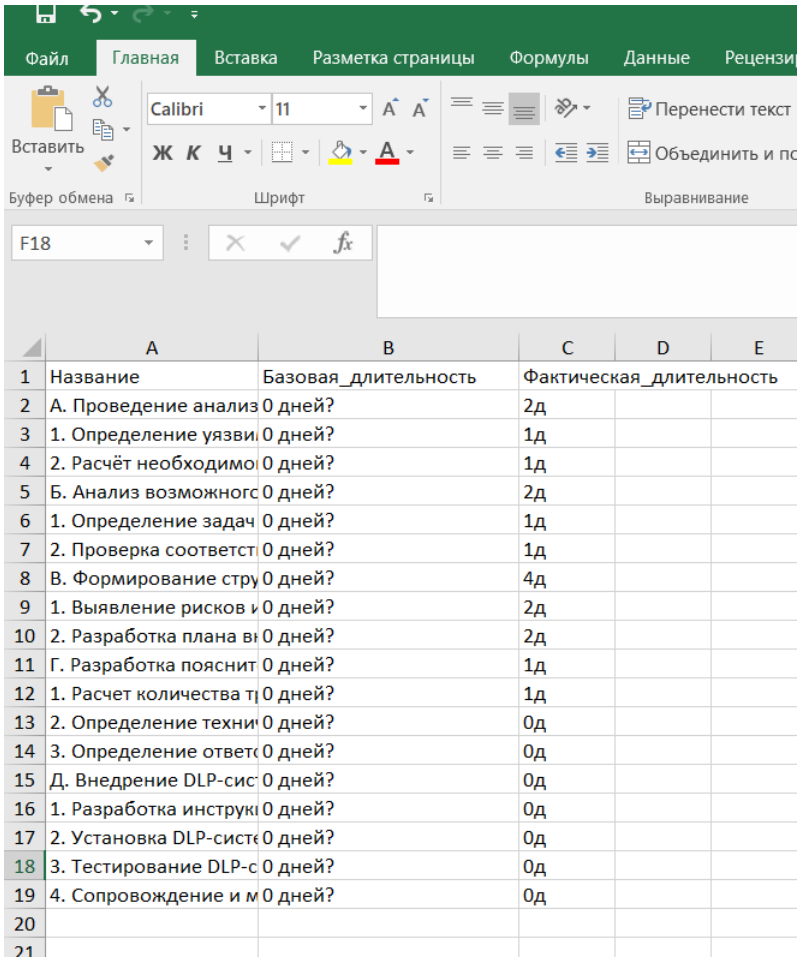


Рисунок – Таблица задач

11. Практическая работа № 36. Презентация проекта

Инструкция для обучающихся

Внимательно прочитайте задание. Разработайте презентацию проекта.

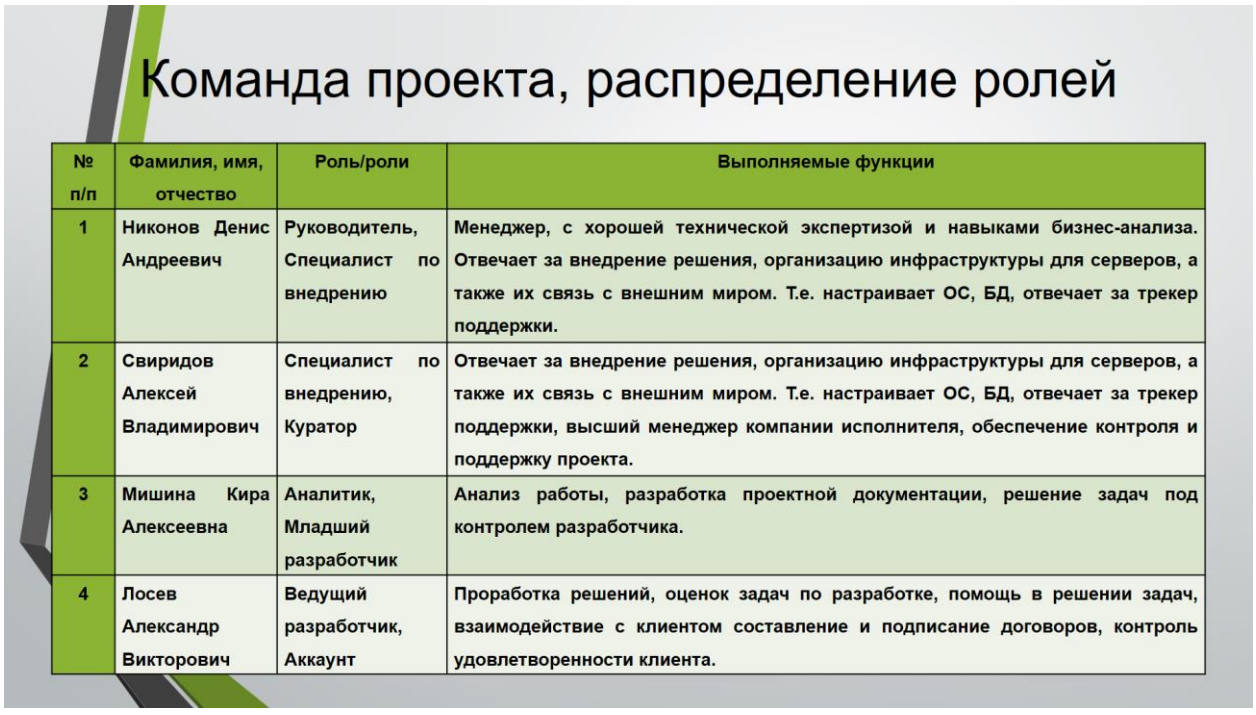
Время выполнения задания – 60 минут.

Задание 1. Подготовьте презентацию по проекту. В презентации должны быть отражены следующие разделы:

- команда проекта;
- идея проекта;
- цели;
- задачи;
- описание произошедшей форс-мажорной ситуации.
- стадии проекта;
- продолжительность проекта по стадиям (скорректированная). Обоснование выбора оптимального метода продолжительности реализации проекта.
- информация о ресурсах;
- стоимость проекта, бюджет;
- плановые и фактические показатели проекта;
- вывод.

Задание 2. Вставьте скриншоты презентации в отчет по практической работе. Прикрепите в СДО отчет (файл .docx) и презентацию проекта (файл .pptx).

Эталон ответа:



Идея проекта

«Разработка и внедрение DLP-системы Infoprotect»

Организация ООО «Окта», которая занимается разработкой программного обеспечения в области электронного документооборота.

Организация за 3 месяца столкнулась с тем, что были утеряны документы, содержащие коммерческую тайну, а так же утечка информации из клиентской базы организации.

После таких случаев руководитель решил внедрить DLP - систему и обратился с этим запросом к нам в организацию.

Идея проекта

«Разработка и внедрение DLP-системы Infoprotect»

Описание проблемы:

- Проблема состоит в том, что конфиденциальная информация имеющая ценность для организации может быть утеряна;
- Проблема затрагивает разного рода ситуации, когда сотрудники организации своими умышленными и неумышленными действиями утрачивают или распространяют конфиденциальную информацию;
- Это приводит к тому, что организация может понести значительный материальный и нематериальный ущерб;
- Удачным решением была бы установка в организации DLP-системы, которая предотвращает утечку информации используя полный набор механизмов контекстного контроля операций с данными, а также технологии их контентной фильтрации.

Идея проекта

Характеристика продукта:

- DLP-система «Infoprotect» представляет собой комплексный программный продукт, цель которого – предотвратить кражу, изменение и распространение конфиденциальной информации;
- Принцип работы DLP-систем «Infoprotect» заключается в анализе всего трафика, который находится в пределах защищаемой корпоративной сети;
- Внедрение DLP-системы «Infoprotect» помогает контролировать входящие и исходящие потоки данных и блокировать попытки несанкционированной передачи важных корпоративных данных.

Цели и задачи проекта

Цели проекта:

- Повышение уровня безопасности бизнес-процессов компании путем внедрения и установки DLP-системы;
- Достичь максимального уровня производительности и эффективности установленного программного обеспечения;
- Внедрить DLP-систему в организацию с минимальными затратами для неё;
- Провести все мероприятия связанные с внедрением DLP-системы в организацию в срок до 05.11.2020.

Цели и задачи проекта

Задачи проекта:

- Рассмотрение запросов организации;
- Предоставление инструментария для расследования инцидентов: создание архива передаваемой информации с возможностью последующего ретроспективного поиска;
- Установка DLP-системы на 100 ЭВМ организации;
- Тестирование DLP-системы;
- Сопровождение и мониторинг DLP-системы;
- Своевременное выявление инсайдеров: мониторинг подозрительных действий пользователей;
- Оптимизация использования корпоративных информационных ресурсов: пресечение использования ресурсов в личных целях;
- Дальнейшее сопровождение.

Стадии проекта

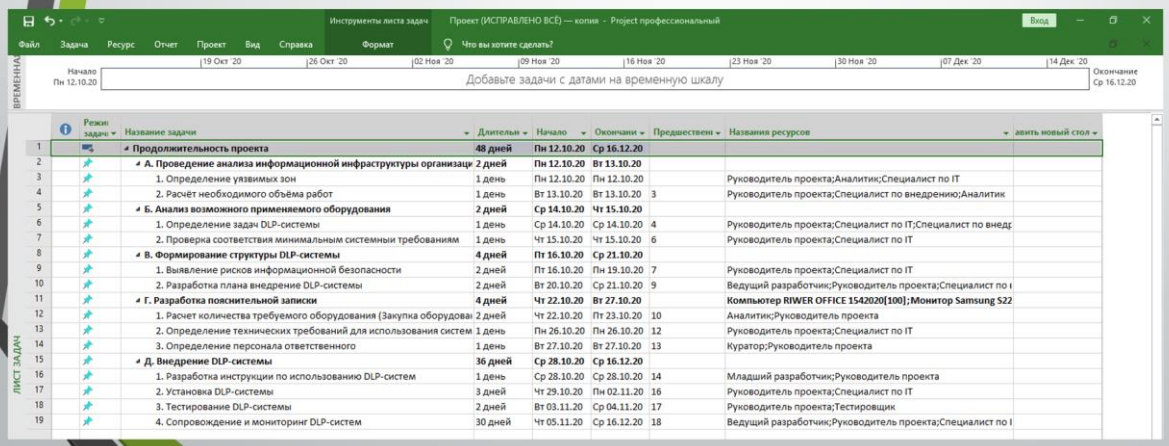
Были определены следующие стадии реализации проекта:

- **А. Проведение анализа информационной инфраструктуры организации:**
  - 1. Определение уязвимых зон
  - 2. Расчёт необходимого объёма работ
- **Б. Анализ возможного применяемого оборудования:**
  - 1. Определение задач DLP-системы
  - 2. Проверка соответствия минимальным системным требованиям
- **В. Формирование структуры DLP-системы:**
  - 1. Выявление рисков информационной безопасности
  - 2. Разработка плана внедрение DLP-системы
- **Г. Разработка пояснительной записки:**
  - 1. Расчет количества требуемого оборудования (Закупка оборудования)
  - 2. Определение технических требований для использования системы
  - 3. Определение ответственного персонала
- **Д. Внедрение DLP-системы:**
  - 1. Разработка инструкции по использованию DLP-системы
  - 2. Установка DLP-системы
  - 3. Тестирование DLP-системы
  - 4. Сопровождение и мониторинг DLP-системы

Продолжительность проекта по стадиям

Общая продолжительность реализации проекта была определена в **48 дней**.

По стадиям длительность проекта была определена следующим образом:



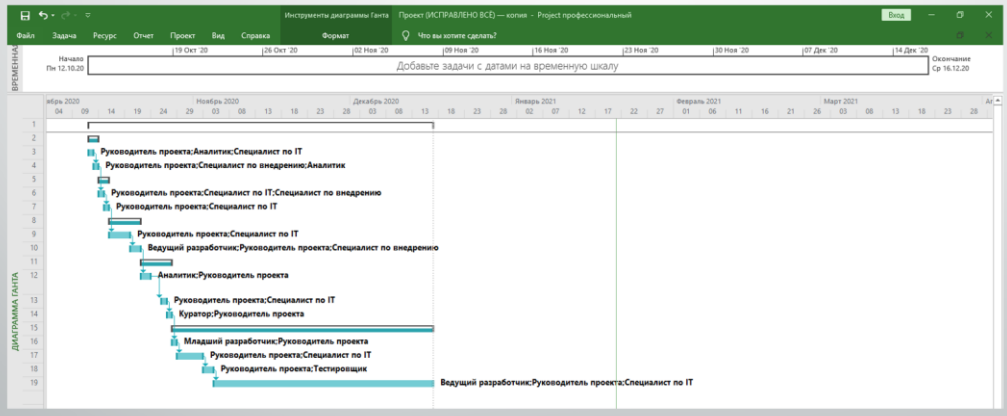
	Режим задач	Название задачи	Длительн	Начало	Окончани	Предшествен	Названия ресурсов
1		**Продолжительность проекта**	**48 дней**	**Пн 12.10.20**	**Ср 16.12.20**		
2		**А. Проведение анализа информационной инфраструктуры организаци**	**2 дней**	**Пн 12.10.20**	**Вт 13.10.20**		
3		1. Определение уязвимых зон	1 день	Пн 12.10.20	Пн 12.10.20		Руководитель проекта;Аналитик;Специалист по IT
4		2. Расчёт необходимого объёма работ	1 день	Вт 13.10.20	Вт 13.10.20	3	Руководитель проекта;Специалист по внедрению;Аналитик
5		**Б. Анализ возможного применяемого оборудования**	**2 дней**	**Ср 14.10.20**	**Чт 15.10.20**		
6		1. Определение задач DLP-системы	1 день	Ср 14.10.20	Ср 14.10.20	4	Руководитель проекта;Специалист по IT;Специалист по внедр
7		2. Проверка соответствия минимальным системным требованиям	1 день	Чт 15.10.20	Чт 15.10.20	6	Руководитель проекта;Специалист по IT
8		**В. Формирование структуры DLP-системы**	**4 дней**	**Пт 16.10.20**	**Ср 21.10.20**		
9		1. Выявление рисков информационной безопасности	2 дней	Пт 16.10.20	Пн 19.10.20	7	Руководитель проекта;Специалист по IT
10		2. Разработка плана внедрение DLP-системы	2 дней	Вт 20.10.20	Ср 21.10.20	9	Ведущий разработчик;Руководитель проекта;Специалист по
11		**Г. Разработка пояснительной записки**	**4 дней**	**Чт 22.10.20**	**Вт 27.10.20**		**Компьютер RIWER OFFICE 1542020[100];Монитор Samsung S22**
12		1. Расчет количества требуемого оборудования (Закупка оборудова	2 дней	Чт 22.10.20	Пт 23.10.20	10	Аналитик;Руководитель проекта
13		2. Определение технических требований для использования систем	1 день	Пн 26.10.20	Пн 26.10.20	12	Руководитель проекта;Специалист по IT
14		3. Определение персонала ответственного	1 день	Вт 27.10.20	Вт 27.10.20	13	Куратор;Руководитель проекта
15		**Д. Внедрение DLP-системы**	**36 дней**	**Ср 28.10.20**	**Ср 16.12.20**		
16		1. Разработка инструкции по использованию DLP-систем	1 день	Ср 28.10.20	Ср 28.10.20	14	Младший разработчик;Руководитель проекта
17		2. Установка DLP-системы	3 дней	Чт 29.10.20	Пн 02.11.20	16	Руководитель проекта;Специалист по IT
18		3. Тестирование DLP-системы	2 дней	Вт 03.11.20	Ср 04.11.20	17	Руководитель проекта;Тестировщик
19		4. Сопровождение и мониторинг DLP-систем	30 дней	Чт 05.11.20	Ср 16.12.20	18	Ведущий разработчик;Руководитель проекта;Специалист по

Трудовые ресурсы

Трудовые ресурсы				
Наименование	Количество	Ставка сверхурочных	Стандартная ставка	Затраты
Руководитель проекта	1	187,50 ₽/ч	562,50 ₽/ч	216 000,00 ₽
Аналитик	1	129,00 ₽/ч	387,50 ₽/ч	12 400,00 ₽
Ведущий разработчик	1	160,00 ₽/ч	479,00 ₽/ч	122 624,00 ₽
Младший разработчик	1	97,00 ₽/ч	291,00 ₽/ч	2 328,00 ₽
Специалист по внедрению	2	136,00 ₽/ч	408,00 ₽/ч	13 056,00 ₽
Куратор	1	93,00 ₽/ч	279,00 ₽/ч	2 232,00 ₽
Специалист по IT	1	71,00 ₽/ч	212,50 ₽/ч	66 300,00 ₽
Тестировщик	2	99,00 ₽/ч	296,90 ₽/ч	4 750,40 ₽
Итого	10			439 690,40 ₽

Графическое отображение реализации проекта

Итоговое графическое изображение реализации проекта:



Материальные ресурсы (до изменения цены)

Материальные ресурсы			
Наименование	Количество	Стоимость	Затраты
Компьютер RIWER OFFICE 1542020 https://www.ironbook.ru/catalog/computers/1542020/	100	19 428,00 ₽	1 942 800,00 ₽
Монитор Samsung S22B300N https://www.ittelo.ru/partsittelo/monitory/Samsung-S22B300N	101	5 000,00 ₽	505 000,00 ₽
Сервер HP Proliant DL360 Gen10 (P19178-B21) https://www.regard.ru/catalog/tovar334427.htm	1	361 560,00 ₽	361 560,00 ₽
Итого	202		2 809 360 ₽

Описание форс-мажорной ситуации

Возросла стоимость закупаемого оборудования на 10%

До наступления ситуации затраты на оборудование составляли:

Название ресурса	Тип	Единицы измерения материалов	Краткое названи	Группа	Макс. едини	Ставка сверхуроч	Стандартна ставка	Начисление	Базовый календарь	Код	Затраты	авить
Компьютер RIWER OFFICE 1542020	Материальны		К				19 428,00 ₽	В начале			1 942 800,00 ₽	
Монитор Samsung S22B300N	Материальны		М				5 000,00 ₽	В начале			505 000,00 ₽	
Сервер HP Proliant DL360 Gen10 (P19178-B21)	Материальны		С				361 560,00 ₽	В начале			361 560,00 ₽	

Для решения возникшей ситуации было принято решение увеличить затраты на закупаемое оборудование на 10%.

2 809 360 руб. – общая стоимость оборудования до изменения цены

Итоговая цена:

Название ресурса	Тип	Единицы измерения материалов	Краткое названи	Группа	Макс. едини	Ставка сверхуроч	Стандартна ставка	Начисление	Базовый календарь	Код	Затраты	авить новы
Компьютер RIWER OFFICE 1542020	Материальны		К				21 370,80 ₽	В начале			2 137 080,00 ₽	
Монитор Samsung S22B300N	Материальны		М				5 500,00 ₽	В начале			555 500,00 ₽	
Сервер HP Proliant DL360 Gen10 (P19178-B21)	Материальны		С				397 716,00 ₽	В начале			397 716,00 ₽	

3 090 296 руб. – общая стоимость оборудования после изменения цены

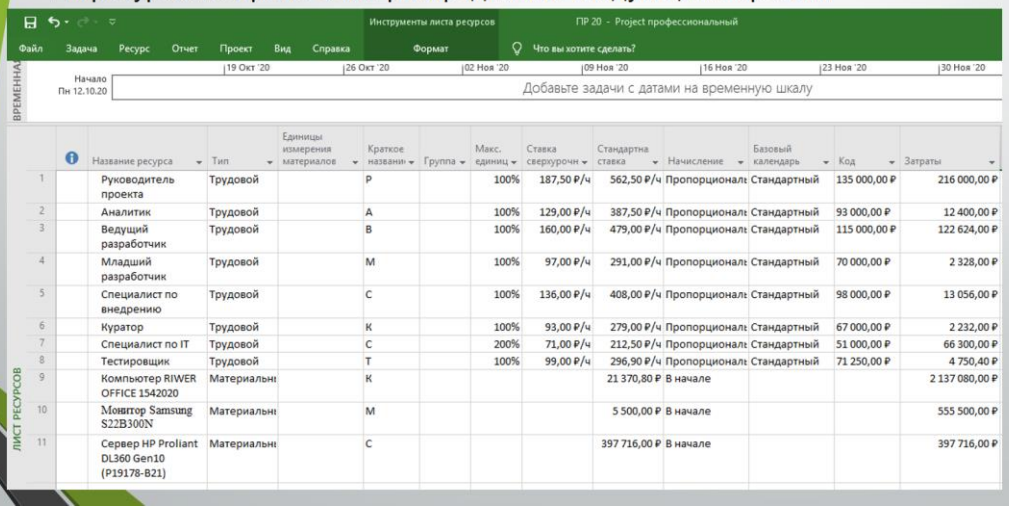
Материальные ресурсы (после изменения цены)

Материальные ресурсы			
Наименование	Количество	Стоимость	Затраты
Компьютер RIWER OFFICE 1542020 https://www.ironbook.ru/catalog/computers/1542020/	100	21 370,80 ₽	2 137 080,00 ₽
Монитор Samsung S22B300N https://www.ittelo.ru/partsittelo/monitory/Samsung-S22B300N	101	5 500,00 ₽	555 500,00 ₽
Сервер HP Proliant DL360 Gen10 (P19178-B21) https://www.regard.ru/catalog/tovar334427.htm	1	397 716,00 ₽	397 716,00 ₽
Итого	202		3 090 296 ₽

Бюджет проекта

Общая сумма затрат составила **3 529 986 рублей 40 копеек**.

По ресурсам затраты были распределены следующим образом:



	Название ресурса	Тип	Единицы измерения материалов	Краткое названи	Группа	Макс. единиц	Ставка сверхурочн	Стандартна ставка	Начисление	Базовый календарь	Код	Затраты
1	Руководитель проекта	Трудовой		Р		100%	187,50 ₽/ч	562,50 ₽/ч	Пропорциональ	Стандартный	135 000,00 ₽	216 000,00 ₽
2	Аналитик	Трудовой		А		100%	129,00 ₽/ч	387,50 ₽/ч	Пропорциональ	Стандартный	93 000,00 ₽	12 400,00 ₽
3	Ведущий разработчик	Трудовой		В		100%	160,00 ₽/ч	479,00 ₽/ч	Пропорциональ	Стандартный	115 000,00 ₽	122 624,00 ₽
4	Младший разработчик	Трудовой		М		100%	97,00 ₽/ч	291,00 ₽/ч	Пропорциональ	Стандартный	70 000,00 ₽	2 328,00 ₽
5	Специалист по внедрению	Трудовой		С		100%	136,00 ₽/ч	408,00 ₽/ч	Пропорциональ	Стандартный	98 000,00 ₽	13 056,00 ₽
6	Куратор	Трудовой		К		100%	93,00 ₽/ч	279,00 ₽/ч	Пропорциональ	Стандартный	67 000,00 ₽	2 232,00 ₽
7	Специалист по IT	Трудовой		С		200%	71,00 ₽/ч	212,50 ₽/ч	Пропорциональ	Стандартный	51 000,00 ₽	66 300,00 ₽
8	Тестировщик	Трудовой		Т		100%	99,00 ₽/ч	296,90 ₽/ч	Пропорциональ	Стандартный	71 250,00 ₽	4 750,40 ₽
9	Компьютер RIWER OFFICE 1542020	Материальн		К				21 370,80 ₽	В начале			2 137 080,00 ₽
10	Монитор Samsung S22B300N	Материальн		М				5 500,00 ₽	В начале			555 500,00 ₽
11	Сервер HP Proliant DL360 Gen10 (P19178-B21)	Материальн		С				397 716,00 ₽	В начале			397 716,00 ₽

Плановые и фактические показатели проекта

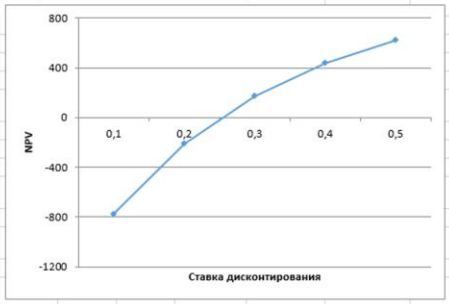
Плановые показатели проекта:

Инвестиционная компания рассматривает проект внедрения новой компьютерной установки:
предполагается вложить в производство 1600 тыс. руб.,
получить в течение первого года 10000 тыс. руб. дохода, исчерпав ресурсы компании,
и в течение второго года внедрить дополнительные ресурсы,
вложив в это 10000 тыс. руб. Постройте график функции NPV(Y) этого проекта.

Безрисковая ставка равна		10%	
Период - год	0	1	2
Оттоки (-E)	-1600		-10000
Притоки (I)		10000	
Денежный поток (CF)	-1600	10000	-10000
Внутренняя норма рентабельности (IRR)	25%		
Норма прибыли (ARR)	-7%		

Зависимость NPV от норма отдачи (Y)					
Норма отдачи (Y)	10%	20%	30%	40%	50%
Чистая текущая стоимость (NPV)	-773,55р.	-211,11р.	175,15р.	440,82р.	622,22р.

Текущая стоимость оттоков PV(-E)	-9 864,46р.		
Период	0	1	2
Модифицированные денежные потоки для MIRR	-9 864,46р.	10 000,00р.	0,00р.
Модифицированная внутренняя норма рентабельности (MIRR)	1%		



Плановые и фактические показатели проекта

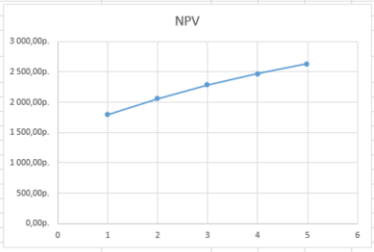
Фактические показатели проекта:

Инвестиционная компания рассматривает проект внедрения новой компьютерной установки:
предполагается вложить в производство 1600 тыс. руб.,
получить в течение первого года 10000 тыс. руб. дохода, исчерпав ресурсы компании,
и в течение второго года внедрить дополнительные ресурсы,
вложив в это 10000 тыс. руб. Необходимо построить график функции NPV(Y) этого проекта.

Безрисковая ставка равна		10%	
Период - год	Октябрь	Ноябрь	Декабрь
Оттоки (-E)	-3202	-166	-160
Притоки (I)			5000
Денежный поток (CF)	-3202	-166	4 840,00р.
Внутренняя норма рентабельности (IRR)	20%		
Норма прибыли (ARR)	22%		

Зависимость NPV от норма отдачи (Y)					
Норма отдачи (Y)	10%	20%	30%	40%	50%
Чистая текущая стоимость (NPV)	1 791,90р.	2 056,39р.	2 278,70р.	2 468,16р.	2 631,56р.

Текущая стоимость оттоков PV(-E)	798,00р.		
Период	0	1	2
Модифицированные денежные потоки для MIRR	798,00р.	-166,00р.	-160,00р.
Модифицированная внутренняя норма рентабельности (MIRR)	-44%		



3.3. Контрольно-оценочные материалы для промежуточной аттестации

Формой промежуточной аттестации по МДК.05.01 является дифференцированный зачет.

Перечень экзаменационных вопросов:
1. Основные понятия информационной безопасности.
2. Угрозы информационной безопасности в информационных системах.
3. Оценочные стандарты в информационной безопасности.
4. Стандарты управления информационной безопасностью.
5. Создание СУИБ на предприятии.
6. Методика оценки рисков информационной безопасности компании Digital Security.
7. Методики и технологии управления рисками.
8. Разработка корпоративной методики анализа рисков.
9. Современные методы и средства анализа и управление рисками информационных систем
компаний.
10.Правовые меры обеспечения информационной безопасности.
11.Организационные меры обеспечения безопасности компьютерных информационных систем.
12.Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом.
13.Протоколирование и аудит, шифрование, контроль целостности.

Эталон ответов: приведен в Учебном пособии по МДК.05.01
Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 30 минут
3. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Формой промежуточной аттестации по МДК.05.02 является дифференциальный зачет.

Перечень вопросов для дифференциального зачета:
1. Задачи, функции и структура подразделений защиты информации
2. Принципы создания и деятельности подразделения защиты информации
3. Критерии подбора и расстановки сотрудников подразделений защиты информации
4. Перечень знаний, необходимых знаний для должности Техник по защите информации, в соответствии с профессиональным стандартом Специалист по защите информации в автоматизированных системах

5. Должностные обязанности техника по защите информации в соответствии с профессиональным стандартом Специалист по защите информации в автоматизированных системах.
6. Методы и технология управления подразделений по защите информации
7. Методы проверки персонала по защите информации
8. Контроль соблюдения персоналом требований режима защиты информации и обучение персонала соблюдению требований режима защиты информации
9. Процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией
10. Использование DLP-систем при обнаружении и реагировании на инциденты информационной безопасности
11. Понятие разрешительной системы доступа к конфиденциальной информации. Требования к разрешительной системе доступа к конфиденциальной информации.
12. Управление допуском и доступом в рамках разрешительной системы доступа к конфиденциальной информации.
13. Положение о разрешительной системе доступа к конфиденциальной информации, содержание основных разделов.
14. Экспертная комиссия по защите конфиденциальной информации.
15. Персонал как основная опасность утраты конфиденциальной информации. Периметр защиты. Основные каналы утечки информации.
16. Учет персонала, получившего доступ к конфиденциальной информации. Номенклатура должностей сотрудников, подлежащих оформлению на допуск к конфиденциальной информации.
17. Организация и проведение совещаний и переговоров по конфиденциальным вопросам.
18. Организация работы по защите конфиденциальной информации при осуществлении международного сотрудничества.
19. Требования режима защиты информации при приеме посетителей.
20. Защита конфиденциальной информации при рекламной и публикаторской деятельности

Эталон ответов: приведен в Учебном пособии по МДК 05.02

Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 20 минут
3. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Формой промежуточной аттестации по МДК.05.03 является дифференциальный зачет.

Перечень вопросов для дифференциального зачета:

1. 1. Форензика: определение, классификация, цели и задачи.
2. 2. Компьютерная экспертиза: определение, классификация, используемое ПО.
3. 3. Виды и архитектура СОРМ.
4. 4. Устройство hdd, ssd и flash накопителей.
5. 5. Способы и средства анализа файловых систем.
6. 6. Программные и аппаратные средства копирования носителей информации.
7. 7. RAM-память: устройство, инструментальные средства копирования и анализа.
8. 8. Анализ систем под управлением ОС Windows.
9. 9. Анализ систем под управлением ОС Linux.
10. 10. Межсетевые экраны.
11. 11. Системы обнаружения и предотвращения вторжений.
12. 12. SIEM-системы.
13. 13. Аудит событий ОС Linux.
14. 14. Аудит событий ОС Windows.
15. 15. Методы и способы выявления сетевых атак на основе анализа трафика.
16. 16. Способы и средства восстановление данных.
17. 17. Способы и средства извлечения и анализа метаданные файлов.
18. 18. Этапы проведения компьютерных экспертиз.

Эталон ответов: приведен в Учебном пособии по МДК 05.03

Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 20 минут
3. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Формой промежуточной аттестации по МДК 05.04 и МДК 05.05 является комплексный экзамен.

Перечень экзаменационных вопросов:

№	Перечень теоретических вопросов
1.	Основные положения контрактной системы. Правовое положение заказчика. Требования к участникам закупок.
2.	Национальный режим и импортозамещение в закупках.
3.	Планирование и обоснование закупок. Нормирование. План-график. Отчетность
4.	Общие предписания к осуществлению закупок. Требования к участникам закупок
5.	Преимущества отдельным участникам. Описание объекта закупок. Техническое задание
6.	Функции, права, обязанности и полномочия контрактной службы. Положение о контрактной службе. Должностные инструкции, обязанности сотрудников.
7.	Требования профессиональных стандартов к сотрудникам контрактной службы/контрактным управляющим и к членам закупочных комиссий. Закупочные комиссии. Требования к составу, квалификации сотрудников. Деятельность комиссии.

8.	Алгоритм конкурса в электронной форме. Последствия признания открытого конкурса в электронной форме несостоявшимся, Последствия признания аукциона несостоявшимся . Последствия признания запроса котировок в электронной форме несостоявшимся Последствия признания запроса предложений несостоявшимся
9.	Алгоритм действий заказчика при осуществлении закупки у единственного поставщика. Случаи закупки у единственного поставщика
10.	Государственный (муниципальный) контракт. Приемка. Экспертиза. Контроль и ответственность заказчика
11.	Проектный менеджмент: понятие, характеристика, ключевые отличия проектного менеджмента от традиционного.
12.	Методы управления проектами: классическое проектное управление, Agile, Scrum, Lean, Kanban, Six Sigma.
13.	Стандарты управления проектами: PMBOK, ICB, ISO 10006, OPM3.
14.	Проект как система. Системный подход к управлению проектами.
15.	Цели проекта. Технология SMART постановки целей проекта. Требования, предъявляемые к проекту.
16.	Окружение проекта. Участники проекта и их роли.
17.	Жизненный цикл и структура проекта.
18.	Основные задачи планирования проекта. Иерархическая структура работ проекта.
19.	Распределение ресурсов. Разработка расписания проекта.
20.	Анализ критического пути проекта: методы НИР, НОФ и МКР определения продолжительности проекта.
21.	Оценка эффективности проекта: стоимость проекта, понятие и этапы оценки эффективности проекта, источники финансирования проекта.
22.	Классификация проектных рисков.
23.	Система управления проектными рисками.
24.	Оценка проектных рисков.
25.	Основные подходы и методы управления рисками.
26.	Управление коммуникациями проекта: роль и виды коммуникаций, планирование управления коммуникациями.
27.	Информационные системы управления проектами: понятие, цели, задачи, функции.
28.	Планирование и обеспечение качества проекта. Контроль качества проекта.
29.	Основные процедуры закрытия проекта, составление окончательного отчета о реализации проекта.
30.	Представление проекта заказчику, оценка проекта по его завершении.

Эталон ответов: приведен в Учебных пособиях МДК.05.04, МДК.05.05.

Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 30 минут
3. Требования к устным ответам:

Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.

4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Критерии оценки устных ответов

В системе оценки знаний и умений используются **следующие критерии**:

«Отлично» – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом за умение связывать теорию с практикой, решать практические задачи, высказывать и обосновывать свои суждения. Отличная отметка предполагает грамотное, логичное изложение ответа (как в устной, так и в письменной форме), качественное внешнее оформление.

«Хорошо» – если обучающийся полно освоил учебный материал, владеет понятийным аппаратом, ориентируется в изученном материале, грамотно излагает ответ, но содержание и форма ответа имеют некоторые неточности.

«Удовлетворительно» – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определение понятий, не умеет доказательно обосновать свои суждения.

«Неудовлетворительно» – если обучающийся имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определение понятий, искажает их смысл, беспорядочно и неуверенно излагает материал, за полное незнание и непонимание учебного материала или отказ отвечать.