

УТВЕРЖДЕНО

Рабочей группой по вопросам
разработки оценочных материалов
в 2021 году для проведения
Демонстрационного экзамена
по стандартам Ворлдскиллс Россия
по образовательным программам
среднего профессионального
образования

Протокол от 23.12.2021г.

№ Пр-23.12.2021-1

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ДЕМОСТРАЦИОННОГО ЭКЗАМЕНА ПО СТАНДАРТАМ ВОРЛДСКИЛЛС РОССИЯ

Номер компетенции	F7
Наименование компетенции	Корпоративная защита от внутренних угроз информационной безопасности

Оглавление

1. Инструкция по охране труда и технике безопасности для проведения Демонстрационного экзамена по стандартам Ворлдскиллс Россия.....	6
Инструкция по охране труда для участников	7
1. Общие требования охраны труда	7
2. Требования охраны труда перед началом выполнения работ	8
3. Требования охраны труда во время выполнения работ	9
4. Требования охраны труда в аварийных ситуациях	11
5. Требование охраны труда по окончании работ	12
Инструкция по охране труда для экспертов.....	13
1. Общие требования охраны труда	13
2. Требования охраны труда перед началом работы	14
3. Требования охраны труда во время работы	14
4. Требования охраны труда в аварийных ситуациях	16
5. Требование охраны труда по окончании выполнения работы.....	17
2. Комплект оценочной документации паспорт КОД 1.1–2022.....	18
Паспорт комплекта оценочной документации	18
1. Описание	18
2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта.....	20
3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке.....	26
4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную	27
5. Список оборудования и материалов, запрещенных на площадке (при наличии).....	27
6. Детальная информация о распределении баллов и формате оценки.....	28
7. Примерный план работы Центра проведения демонстрационного экзамена.	29
8. Необходимые приложения	34

План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный)	35
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (дистанционный)	37
Образец задания	38
3. Комплект оценочной документации паспорт КОД 1.2–2022.....	53
Паспорт комплекта оценочной документации	53
1. Описание	53
2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта	55
3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке.....	59
4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную	60
5. Список оборудования и материалов, запрещенных на площадке (при наличии)	60
6. Детальная информация о распределении баллов и формате оценки.....	61
7. Примерный план работы Центра проведения демонстрационного экзамена.	62
8. Необходимые приложения	66
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный).....	67
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (дистанционный)	69
Образец задания	70
4. Комплект оценочной документации паспорт КОД 1.3–2022.....	79
Паспорт комплекта оценочной документации	79
1. Описание	79
2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта	81
3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке.....	87

4.	Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную	88
5.	Список оборудования и материалов, запрещенных на площадке (при наличии)	88
6.	Детальная информация о распределении баллов и формате оценки.....	89
7.	Примерный план работы Центра проведения демонстрационного экзамена.	90
8.	Необходимые приложения	94
	План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный).....	95
	План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (дистанционный)	97
	Образец задания	98
5.	Комплект оценочной документации паспорт КОД 1.4-2022	109
	Паспорт комплекта оценочной документации	109
1.	Описание	109
2.	Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта.....	111
3.	Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке.....	115
4.	Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную	116
5.	Список оборудования и материалов, запрещенных на площадке (при наличии)	116
6.	Детальная информация о распределении баллов и формате оценки... ..	117
7.	Примерный план работы Центра проведения демонстрационного экзамена.	118
8.	Необходимые приложения	122
	План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный).....	123
	План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (дистанционный)	125

Образец задания	126
6. Комплект оценочной документации паспорт КОД 1.5–2022.....	133
Паспорт комплекта оценочной документации	133
1. Описание	133
2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта.....	135
3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке.....	138
4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную	139
5. Список оборудования и материалов, запрещенных на площадке (при наличии).....	139
6. Детальная информация о распределении баллов и формате оценки...	140
7. Примерный план работы Центра проведения демонстрационного экзамена.	141
8. Необходимые приложения	145
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный).....	146
Образец задания	148
7. Комплект оценочной документации паспорт КОД 2.1–2022.....	156
Паспорт комплекта оценочной документации	156
1. Описание	156
2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта.....	158
3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке.....	166
4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную	167
5. Список оборудования и материалов, запрещенных на площадке (при наличии).....	167
6. Детальная информация о распределении баллов и формате оценки...	168

7. Примерный план работы Центра проведения демонстрационного экзамена.	169
8. Необходимые приложения	175
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный).....	176
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (дистанционный)	178
Образец задания	179

1. Инструкция по охране труда и технике безопасности для проведения Демонстрационного экзамена по стандартам Ворлдскиллс Россия

Программа инструктажа по охране труда и технике безопасности.

1. Общие сведения о месте проведения экзамена, расположении компетенции, времени трансфера до места проживания, расположении транспорта для площадки, особенности питания участников и экспертов, месторасположении санитарно-бытовых помещений, питьевой воды, медицинского пункта, аптечки первой помощи, средств первичного пожаротушения.

2. Время начала и окончания проведения экзаменационных заданий, нахождение посторонних лиц на площадке.

3. Контроль требований охраны труда участниками и экспертами.

4. Вредные и опасные факторы во время выполнения экзаменационных заданий и нахождение на территории проведения экзамена.

5. Общие обязанности участника и экспертов по охране труда, общие правила поведения во время выполнения экзаменационных заданий и на территории.

6. Основные требования санитарии и личной гигиены.

7. Средства индивидуальной и коллективной защиты, необходимость их использования.

8. Порядок действий при плохом самочувствии или получении травмы. Правила оказания первой помощи.

9. Действия при возникновении чрезвычайной ситуации, ознакомление со схемой эвакуации и пожарными выходами.

Инструкция по охране труда для участников

1. Общие требования охраны труда

- К самостоятельному выполнению заданий экзамена по стандартам «WorldSkills» допускаются участники:
 - прошедшие инструктаж по охране труда по «Программе инструктажа по охране труда и технике безопасности»;
 - ознакомленные с инструкцией по охране труда;
 - имеющие необходимые навыки по эксплуатации инструмента, приспособлений совместной работы на оборудовании;
 - не имеющие противопоказаний к выполнению заданий по состоянию здоровья.
- При работе с ПК рекомендуется организация перерывов на через каждые 45 минут работы.
- При работе на ПК могут воздействовать опасные и вредные производственные факторы:
 - физические: повышенный уровень электромагнитного излучения; повышенный уровень статического электричества; повышенная яркость светового изображения; повышенный уровень пульсации светового потока; повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека; повышенный или пониженный уровень освещенности; повышенный уровень прямой и отраженной блескости;
 - психофизиологические: напряжение зрения и внимания; интеллектуальные и эмоциональные нагрузки; длительные статические нагрузки; монотонность труда.
- Запрещается находиться возле ПК в верхней одежде, принимать пищу и курить, употреблять во время выполнения задания алкогольные напитки, а также приходить на площадку в состоянии алкогольного, наркотического или другого опьянения.
- Участник экзамена должен знать месторасположение первичных средств пожаротушения.
- О каждом несчастном случае пострадавший или очевидец несчастного случая немедленно должен известить ближайшего эксперта.
- В помещении экспертов находится аптечка первой помощи, укомплектованная изделиями медицинского назначения, ее необходимо

использовать для оказания первой помощи, самопомощи в случаях получения травмы.

- В случае возникновения несчастного случая или болезни участника, об этом немедленно уведомляются Главный эксперт и линейные Эксперты. Главный эксперт принимает решение о назначении дополнительного времени для участия. В случае отстранения участника от дальнейшего участия в экзамене ввиду болезни или несчастного случая, он получит баллы за любую завершённую работу.
- Вышеуказанные случаи подлежат обязательной регистрации в Форме регистрации несчастных случаев и в Форме регистрации перерывов в работе.
- Знаки безопасности, используемые на рабочем месте, для обозначения присутствующих опасностей:

- F 04 Огнетушитель



- E 22 Указатель выхода



- E 23 Указатель запасного выхода



- ЕС 01 Аптечка первой медицинской помощи



- При работе с ПК участники экзамена должны соблюдать правила личной гигиены.
- Работа на площадке разрешается исключительно в присутствии эксперта. Запрещается присутствие на площадке посторонних лиц.
- По всем вопросам, связанным с работой компьютера, следует обращаться к техническому эксперту.
- Участники, допустившие невыполнение или нарушение инструкции по охране труда, привлекаются к ответственности в соответствии с Регламентом.
- Несоблюдение норм безопасности может привести к временному или перманентному отстранению аналогично апелляции.

2. Требования охраны труда перед началом выполнения работ

- В подготовительный день все участники должны ознакомиться с инструкцией по технике безопасности, с планами эвакуации при возникновении пожара, местами расположения санитарно-бытовых

помещений, медицинскими кабинетами, питьевой воды, подготовить рабочее место в соответствии с Техническим описанием компетенции.

- По окончании ознакомительного периода, участники подтверждают свое ознакомление со всеми процессами, подписав лист прохождения инструктажа по работе на оборудовании по форме, определенной Оргкомитетом.
- Подготовить рабочее место:
 - Осмотреть и привести в порядок рабочее место, убрать все посторонние предметы, которые могут отвлекать внимание и затруднять работу.
 - Проверить правильность установки стола, стула, подставки под ноги, угол наклона экрана монитора, положения клавиатуры в целях исключения неудобных поз и длительных напряжений тела. Особо обратить внимание на то, что дисплей должен находиться на расстоянии не менее 50 см от глаз (оптимально 60-70 см).
 - Проверить правильность расположения оборудования.
 - Кабели электропитания, удлинители, сетевые фильтры должны находиться с тыльной стороны рабочего места, сетевые фильтры не должны лежать на полу.
 - Убедиться в отсутствии засветок, отражений и бликов на экране монитора.
 - Убедиться в том, что на устройствах ПК (системный блок, монитор, клавиатура) не располагаются сосуды с жидкостями, сыпучими материалами (чай, кофе, сок, вода и пр.).
 - Включить электропитание в последовательности, установленной инструкцией по эксплуатации на оборудование; убедиться в правильном выполнении процедуры загрузки оборудования, правильных настройках.

Участнику запрещается приступать к выполнению задания при обнаружении неисправности оборудования. О замеченных недостатках и неисправностях немедленно сообщить Эксперту и до устранения неполадок к заданию не приступать.

3. Требования охраны труда во время выполнения работ

- В течение всего времени выполнения задания со средствами компьютерной и оргтехники участник экзамена обязан:
 - содержать в порядке и чистоте рабочее место;

- следить за тем, чтобы вентиляционные отверстия устройств ничем не были закрыты;
- выполнять требования инструкции по эксплуатации оборудования;
- соблюдать, установленные расписанием, перерывы в выполнении задания, выполнять рекомендованные физические упражнения.
- Участнику запрещается во время выполнения задания:
 - отключать и подключать интерфейсные кабели периферийных устройств если это не указано в задании;
 - класть на устройства средств компьютерной и оргтехники бумаги, папки и прочие посторонние предметы;
 - прикасаться к задней панели системного блока (процессора) при включенном питании;
 - отключать электропитание во время выполнения программы, процесса;
 - допускать попадание влаги, грязи, сыпучих веществ на устройства средств компьютерной и оргтехники;
 - производить самостоятельно вскрытие и ремонт оборудования;
 - работать со снятыми кожухами устройств компьютерной и оргтехники;
 - располагаться при работе на расстоянии менее 50 см от экрана монитора.
- При работе с текстами на бумаге, листы надо располагать как можно ближе к экрану, чтобы избежать частых движений головой и глазами при переводе взгляда.
- Рабочие столы следует размещать таким образом, чтобы экран монитора был ориентирован боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева.
- Освещение не должно создавать бликов на поверхности экрана.
- Продолжительность работы на ПК без регламентированных перерывов не должна превышать 1-го часа. Во время регламентированного перерыва с целью снижения нервно-эмоционального напряжения, утомления зрительного аппарата, необходимо выполнять комплексы физических упражнений.
- При неисправности инструмента и оборудования – прекратить выполнение задания и сообщить об этом Эксперту, а в его отсутствие заместителю главного Эксперта.

4. Требования охраны труда в аварийных ситуациях

- При обнаружении неисправности в работе электрических устройств, находящихся под напряжением (повышенном их нагреве, появления искрения, запаха гари, задымления и т. д.), участнику следует немедленно сообщить о случившемся Экспертам. Выполнение задания продолжить только после устранения возникшей неисправности.
- В случае возникновения у участника плохого самочувствия или получения травмы сообщить об этом эксперту.
- При поражении участника электрическим током немедленно отключить электросеть, оказать первую помощь (самопомощь) пострадавшему, сообщить Эксперту, при необходимости обратиться к врачу.
- При несчастном случае или внезапном заболевании необходимо в первую очередь отключить питание электрооборудования, сообщить о случившемся Экспертам, которые должны принять мероприятия по оказанию первой помощи пострадавшим, вызвать скорую медицинскую помощь, при необходимости отправить пострадавшего в ближайшее лечебное учреждение.
- При возникновении пожара необходимо немедленно оповестить Главного эксперта и экспертов. При последующем развитии событий следует руководствоваться указаниями Главного эксперта или эксперта, заменяющего его. Приложить усилия для исключения состояния страха и паники.
- При обнаружении очага возгорания на площадке необходимо любым возможным способом постараться загасить пламя в "зародыше" с обязательным соблюдением мер личной безопасности.
- При возгорании одежды попытаться сбросить ее. Если это сделать не удастся, упасть на пол и, перекатываясь, сбить пламя; необходимо накрыть горящую одежду куском плотной ткани, облиться водой, запрещается бежать – бег только усилит интенсивность горения.
- В загоревшемся помещении не следует дожидаться, пока приблизится пламя. Основная опасность пожара для человека – дым. При наступлении признаков удушья лечь на пол и как можно быстрее ползти в сторону эвакуационного выхода.
- При обнаружении взрывоопасного или подозрительного предмета не подходите близко к нему, предупредите о возможной опасности находящихся поблизости экспертов или обслуживающий персонал.

- При происшествии взрыва необходимо спокойно уточнить обстановку и действовать по указанию экспертов, при необходимости эвакуации возьмите с собой документы и предметы первой необходимости, при передвижении соблюдайте осторожность, не трогайте поврежденные конструкции, оголившиеся электрические провода. В разрушенном или поврежденном помещении не следует пользоваться открытым огнем (спичками, зажигалками и т. п.).

5. Требование охраны труда по окончании работ

- По окончании работы участник экзамена обязан соблюдать следующую последовательность отключения оборудования:
 - произвести завершение всех выполняемых на ПК задач;
 - отключить питание в последовательности, установленной инструкцией по эксплуатации данного оборудования.
- Убрать со стола рабочие материалы и привести в порядок рабочее место.
- Обо всех замеченных неполадках сообщить эксперту.
- Сообщить эксперту о выявленных во время выполнения заданий неполадках и неисправностях оборудования, и других факторах, влияющих на безопасность выполнения задания.

Инструкция по охране труда для экспертов

1. Общие требования охраны труда

- К работе в качестве эксперта Компетенции «Корпоративная защита от внутренних угроз информационной безопасности» допускаются Эксперты, прошедшие специальное обучение и не имеющие противопоказаний по состоянию здоровья.
- Эксперт с особыми полномочиями, на которого возложена обязанность за проведение инструктажа по охране труда, должен иметь действующее удостоверение «О проверке знаний требований охраны труда».
- В процессе контроля выполнения заданий и нахождения на площадке Эксперт обязан четко соблюдать:
 - инструкции по охране труда и технике безопасности;
 - правила пожарной безопасности, знать места расположения первичных средств пожаротушения и планов эвакуации.
 - расписание и график проведения задания, установленные режимы труда и отдыха.
- При работе на персональном компьютере и копировально-множительной технике на Эксперта могут воздействовать следующие вредные и (или) опасные производственные факторы:
 - электрический ток;
 - статическое электричество, образующееся в результате трения движущейся бумаги с рабочими механизмами, а также при некачественном заземлении аппаратов;
 - шум, обусловленный конструкцией оргтехники;
 - химические вещества, выделяющиеся при работе оргтехники;
 - зрительное перенапряжение при работе с ПК.
- При несчастном случае пострадавший или очевидец несчастного случая обязан немедленно сообщить о случившемся Главному Эксперту.
В помещении Экспертов Компетенции «Корпоративная защита от внутренних угроз информационной безопасности» находится аптечка первой помощи, укомплектованная изделиями медицинского назначения, ее необходимо использовать для оказания первой помощи, самопомощи в случаях получения травмы.
В случае возникновения несчастного случая или болезни Эксперта, об этом немедленно уведомляется Главный эксперт.

- Эксперты, допустившие невыполнение или нарушение инструкции по охране труда, привлекаются к ответственности в соответствии с Регламентом, а при необходимости согласно действующему законодательству.

2. Требования охраны труда перед началом работы

- Перед началом работы Эксперты должны выполнить следующее:
- В подготовительный день, Эксперт с особыми полномочиями, ответственный за охрану труда, обязан провести подробный инструктаж по «Программе инструктажа по охране труда и технике безопасности», ознакомить экспертов и участников с инструкцией по технике безопасности, с планами эвакуации при возникновении пожара, с местами расположения санитарно-бытовых помещений, медицинскими кабинетами, питьевой воды, проконтролировать подготовку рабочих мест участников в соответствии с Техническим описанием компетенции.
- Ежедневно, перед началом работ на площадке и в помещении экспертов необходимо:
 - осмотреть рабочие места экспертов и участников;
 - привести в порядок рабочее место эксперта;
 - проверить правильность подключения оборудования в электросеть;
- Эксперту запрещается приступать к работе при обнаружении неисправности оборудования. О замеченных недостатках и неисправностях немедленно сообщить Техническому Эксперту и до устранения неполадок к работе не приступать.

3. Требования охраны труда во время работы

- Изображение на экранах видеомониторов должно быть стабильным, ясным и предельно четким, не иметь мерцаний символов и фона, на экранах не должно быть бликов и отражений светильников, окон и окружающих предметов.
- Суммарное время непосредственной работы с персональным компьютером и другой оргтехникой в течение дня должно быть не более 6 часов.

Продолжительность непрерывной работы с персональным компьютером и другой оргтехникой без регламентированного перерыва не должна превышать 2-х часов. Через каждый час работы следует делать регламентированный перерыв продолжительностью 15 мин.

- Во избежание поражения током запрещается:
 - прикасаться к задней панели персонального компьютера и другой оргтехники, монитора при включенном питании;
 - допускать попадания влаги на поверхность монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;
 - производить самостоятельно вскрытие и ремонт оборудования;
 - переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;
 - загромождать верхние панели устройств бумагами и посторонними предметами;
 - допускать попадание влаги на поверхность системного блока, монитора, рабочую поверхность клавиатуры, дисководов, принтеров и др. устройств;
- При выполнении модулей задания участниками, Эксперту необходимо быть внимательным, не отвлекаться посторонними разговорами и делами без необходимости, не отвлекать других Экспертов и участников.
- Эксперту во время работы с оргтехникой:
 - обращать внимание на символы, высвечивающиеся на панели оборудования, не игнорировать их;
 - не снимать крышки и панели, жестко закрепленные на устройстве. В некоторых компонентах устройств используется высокое напряжение или лазерное излучение, что может привести к поражению электрическим током или вызвать слепоту;
 - не производить включение/выключение аппаратов мокрыми руками;
 - не ставить на устройство емкости с водой, не класть металлические предметы;
 - не эксплуатировать аппарат, если он перегрелся, стал дымиться, появился посторонний запах или звук;
 - не эксплуатировать аппарат, если его уронили или корпус был поврежден;
 - вынимать застрявшие листы можно только после отключения устройства из сети;
 - запрещается перемещать аппараты включенными в сеть;
 - все работы по замене картриджей, бумаги можно производить только после отключения аппарата от сети;
 - обязательно мыть руки теплой водой с мылом после каждой чистки картриджей, узлов и т. д.;

- просыпанный тонер, носитель немедленно собрать пылесосом или влажной ветошью.
- Включение и выключение персонального компьютера и оргтехники должно проводиться в соответствии с требованиями инструкции по эксплуатации.
- Запрещается:
 - устанавливать неизвестные системы паролирования и самостоятельно проводить переформатирование диска;
 - иметь при себе любые средства связи;
 - пользоваться любой документацией кроме предусмотренной заданием.
- При неисправности оборудования – прекратить работу и сообщить об этом Техническому эксперту, а в его отсутствие заместителю главного Эксперта.
- При нахождении на площадке Эксперту:
 - одеть необходимые средства индивидуальной защиты;
- передвигаться по площадке не спеша, не делая резких движений, смотря под ноги.

4. Требования охраны труда в аварийных ситуациях

- При обнаружении неисправности в работе электрических устройств, находящихся под напряжением (повышенном их нагреве, появления искрения, запаха гари, задымления и т.д.), Эксперту следует немедленно отключить источник электропитания и принять меры к устранению неисправностей, а также сообщить о случившемся Техническому Эксперту. Выполнение задания продолжать только после устранения возникшей неисправности.
- В случае возникновения зрительного дискомфорта и других неблагоприятных субъективных ощущений следует ограничить время работы с персональным компьютером и другой оргтехникой, провести коррекцию длительности перерывов для отдыха или провести смену деятельности на другую, не связанную с использованием персонального компьютера и другой оргтехники.
- При поражении электрическим током немедленно отключить электросеть, оказать первую помощь (самопомощь) пострадавшему, сообщить Главному Эксперту, при необходимости обратиться к врачу.

- При возникновении пожара необходимо немедленно оповестить Главного эксперта. При последующем развитии событий следует руководствоваться указаниями Главного эксперта или должностного лица, заменяющего его. Приложить усилия для исключения состояния страха и паники.
- При обнаружении очага возгорания на площадке необходимо любым возможным способом постараться загасить пламя в «зародыше» с обязательным соблюдением мер личной безопасности.
- При возгорании одежды попытаться сбросить ее. Если это сделать не удастся, упасть на пол и, перекатываясь, сбить пламя; необходимо накрыть горящую одежду куском плотной ткани, облиться водой, запрещается бежать – бег только усилит интенсивность горения.
- В загоревшемся помещении не следует дожидаться, пока приблизится пламя. Основная опасность пожара для человека – дым. При наступлении признаков удушья лечь на пол и как можно быстрее ползти в сторону эвакуационного выхода.
- При обнаружении взрывоопасного или подозрительного предмета не подходить близко к нему, предупредить о возможной опасности находящихся поблизости ответственных лиц.
- При происшествии взрыва необходимо спокойно уточнить обстановку и действовать по указанию должностных лиц, при необходимости эвакуации, эвакуировать участников и других экспертов и площадки, взять те с собой документы и предметы первой необходимости, при передвижении соблюдать осторожность, не трогать поврежденные конструкции, оголившиеся электрические провода. В разрушенном или поврежденном помещении не следует пользоваться открытым огнем (спичками, зажигалками и т. п.).

5. Требование охраны труда по окончании выполнения работы

- После окончания дня Эксперт обязан:
 - Отключить электрические приборы, оборудование, инструмент и устройства от источника питания.
 - Привести в порядок рабочее место Эксперта и проверить рабочие места участников.
 - Сообщить Техническому эксперту о выявленных во время выполнения заданий неполадках и неисправностях оборудования, и других факторах, влияющих на безопасность труда.

2. Комплект оценочной документации паспорт КОД 1.1– 2022

Паспорт комплекта оценочной документации

1. Описание

Комплект оценочной документации (КОД) разработан в целях организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия.

В данном разделе указаны основные характеристики КОД и должны использоваться при планировании, проведении и оценки результатов демонстрационного экзамена образовательными организациями, ЦПДЭ и Агентством.

Таблица 1. Паспорт комплекта оценочной документации (КОД)

№ п/п	Наименование	Информация о разработанном КОД
1	2	3
1	Номер компетенции	F7
2	Название компетенции	Корпоративная защита от внутренних угроз информационной безопасности
3	КОД является однодневным или двухдневным:	Однодневный
4	Номер КОД	КОД 1.1
4.1	Год(ы) действия КОД	2022 (1 год)
5	Уровень ДЭ	ФГОС СПО
6	Общее максимально возможное количество баллов задания по всем критериям оценки	54,00
7	Длительность выполнения экзаменационного задания данного КОД	6:00:00
8	КОД разработан на основе	ФНЧ Молодые профессионалы 2021
9	КОД подходит для проведения демонстрационного экзамена в качестве процедуры Независимой оценки квалификации (НОК)	НЕТ
10	Вид аттестации, для которой подходит данный КОД	ГИА, Промежуточная
11	Формат проведения ДЭ	X
11.1	КОД разработан для проведения ДЭ в очном формате, (участники и эксперты находятся в ЦПДЭ)	Да
11.2	КОД разработан для проведения ДЭ в дистанционном формате, (участники и эксперты работают удаленно)	Да
11.3	КОД разработан для проведения ДЭ в распределенном формате, (детализация в п.11.3.1)	Да
11.3.1	Формат работы в распределенном формате	Участники находятся в ЦПДЭ, эксперты работают удаленно
12	Форма участия (индивидуальная, парная, групповая)	Индивидуальная

12.1	Количество человек в группе, (т.е. задание ДЭ выполняется индивидуально или в группе/ команде из нескольких экзаменуемых)	1,00
12.2	Организация работы при невозможности разбить экзаменуемых на указанное в п. 12.1 количество человек в группе	
13	Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3,00
16	Автоматизированная оценка результатов заданий	Частичная автоматизация
16.1	Что автоматизировано: заполняется при выборе вариантов в п.16: возможна частичная или полная автоматизация	Модуль 3 (в зависимости от возможностей площадки)

2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта

Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта, (WorldSkills Standards Specification WSSS), проверяемый в рамках комплекта оценочной документации, (Таблица 2).

Таблица 2. WSSS

Номер раздела WSSS	Наименование раздела WSSS	Содержание раздела WSSS: Специалист должен знать	Важность раздела WSSS (%)
1	2	3	4
2	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	<p>Специалист должен знать и понимать:</p> <p>Сетевое окружение;</p> <p>Сетевые протоколы;</p> <p>Знать методы выявления и построения путей движения информации в организации;</p> <p>Подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;</p> <p>Типы сетевых устройств;</p> <p>Разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз;</p> <p>Процесс выбора подходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем;</p> <p>Важность следования инструкциям и последствия, цену пренебрежения ими;</p> <p>Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы;</p> <p>Этапы установки системы корпоративной защиты от внутренних угроз;</p> <p>Знать отличия различных версий систем корпоративной защиты от внутренних угроз;</p> <p>Знать какие СУБД поддерживаются системой;</p> <p>Знать назначение различных компонент версий систем корпоративной защиты от внутренних угроз;</p> <p>Знать технологии программной и аппаратной виртуализации;</p> <p>Знать особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation;</p> <p>Цель документирования процессов обновления и установки.</p> <p>Важность спокойного и сфокусированного подхода к решению проблемы;</p>	14,00

		<p>Значимость систем ИТ-безопасности и зависимость пользователей и организаций от их доступности; Популярные аппаратные и программные ошибки; Знать разделы системы корпоративной безопасности, которые обычно использует системный администратор; Аналитический и диагностический подходы к решению проблем; Границы собственных знаний, навыков и полномочий; Ситуации, требующие вмешательства службы поддержки; Стандартное время решения наиболее популярных проблем. Специалист должен уметь: Интерпретировать пользовательские запросы и требования с точки зрения корпоративных требований; Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении; Настраивать сетевые устройства; Администрирование автоматизированных технические средства управления и контроля информации и информационных потоков; Навыки системного администрирования в операционных системах , Server, Linux (Red Hat Enterprise Linux, CentOS и др.); Навыки системного администрирования в защищенных операционных системах (AstraLinux и др.); Настройка в операционных системах прав доступа в соответствие с ролевой и/или мандатной моделью; Настройка средств виртуализации под операционными системам; Конфигурирование операционных систем для правильного и защищенного использования средств безопасности, в т.ч. системы корпоративной защиты от внутренних угроз.: Установка серверной части системы корпоративной защиты от внутренних угроз; Установка СУБД различного вида; Установка агентской части системы корпоративной защиты от внутренних угроз; Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом; Использовать дополнительные утилиты если это необходимо; Уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки; Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае</p>	
--	--	---	--

		<p>необходимости;</p> <p>Уметь сконфигурировать систему, чтобы она получала теневые копии;</p> <p>Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах;</p> <p>Демонстрировать уверенность и упорство в решении проблем;</p> <p>Быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы, точно описывать проблему и документировать её решение;</p> <p>Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей;</p> <p>Выбирать и принимать диагностирующее ПО и инструменты для поиска неисправностей;</p>	
4	<p>Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз</p>	<p>Специалист должен знать и понимать:</p> <p>Технологии работы с политиками информационной безопасности;</p> <p>Создание новых политик, модификация существующих;</p> <p>Общие принципы при работе интерфейсом системы защиты корпоративной информации;</p> <p>Объекты защиты, персоны;</p> <p>Ключевые технологии анализа трафика;</p> <p>Типовые протоколы и потоки данных в корпоративной среде, такими как:</p> <p>корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4)</p> <p>веб-почта;</p> <p>Интернет-ресурсы: сайты, блоги, форумы и т. д. (протоколы HTTP, HTTPS);</p> <p>социальные сети;</p> <p>интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP;</p> <p>принтеры: печать файлов на локальных и сетевых принтерах;</p> <p>любые съемные носители и устройства;</p> <p>Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек;</p> <p>Типы угроз информационной безопасности, типы инцидентов,</p> <p>Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;</p> <p>Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации;</p> <p>Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;</p> <p>Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения</p>	18,00

		<p>и передачи корпоративной информации;</p> <p>Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки;</p> <p>Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе;</p> <p>Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов;</p> <p>Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации;</p> <p>Специалист должен уметь:</p> <p>Создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты;</p> <p>Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты;</p> <p>Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии;</p> <p>Работа со сводками, виджетами, сводками;</p> <p>Работа с персонами;</p> <p>Работа с объектами защиты;</p> <p>Провести имитацию процесса утечки конфиденциальной информации в системе;</p> <p>Создать непротиворечивые политики, соответствующие нормативной базе и законодательству;</p> <p>Задokumentировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации.</p> <p>Работа с категориями и терминами;</p> <p>Использование регулярных выражений;</p> <p>Использование морфологического поиска;</p> <p>Работа с графическими объектами;</p> <p>Работа с выгрузками и баз данных;</p> <p>Работа с печатями и бланками;</p> <p>Работа с файловыми типами;</p> <p>Эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;</p>	
6	Технологии защиты узла и агентского мониторинга	<p>Специалист должен знать и понимать:</p> <p>Функции агентского мониторинга;</p> <p>Общие настройки системы агентского мониторинга;</p> <p>Соединение с LDAP-сервером и синхронизация с Active Directory или функциональным аналогом;</p>	18,00

		<p>Политики агентского мониторинга, особенности их настройки; Особенности настроек событий агентского мониторинга; Механизмы диагностики агента, подходы к защите агента. Знать возможности и ограничения современных российских и зарубежных операционных систем в рамках решения задач защиты информации Знать архитектуру операционных систем Знать инструментарий по работа с современными операционными системами, команды, ПО. утилиты Специалист должен уметь: Установка и настройка агентского мониторинга; Создание политик защиты на агентах; Работа в консоли управления агентом; Фильтрация событий; Настройка совместных событий агентского и сетевого мониторинга; Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата. Производить настройку сервисов и компонент операционной системы для достижения целей защиты Разделять компоненты операционной системы по уровням доверия, сокращая поверхность атаки для злоумышленника Применять механизмы ролевого и мандатного доступа и контроля целостности Реализовывать ограниченную программную среду для пользователя Знать особенности безопасной работы и загрузки операционных систем на различных аппаратных платформах</p>	
7	Предотвращение инцидентов и управление событиями информационной безопасности	<p>Специалист должен знать и понимать: Назначение, роль, возможности систем IDS/IPS для задачи защиты организации от угроз информационной безопасности Назначение, роль, возможности систем SIEM для задачи защиты организации от угроз информационной безопасности Назначение, роль, возможности систем Threat Intelligence для задачи защиты организации от угроз информационной безопасности Специалист должен уметь: Устанавливать, настраивать системы IDS/IPS Устанавливать, настраивать системы SIEM</p>	4,00

		Устанавливать, настраивать системы Threat Intelligence, генерации трафика и проверки защищенности Применять на практике системы IDS/IPS для выявления инцидентов информационной безопасности Применять на практике системы Threat Intelligence Применять на практике системы Threat Intelligence и Attack Simulation (Breach and Attack Simulation) для проверки/оценки устойчивости систем и сетей к компьютерным атакам Проводить анализ выявленных инцидентов, использовать встроенные и внешние системы подготовки отчетности	
--	--	---	--

*Таблица соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами доступна в Приложении 2.

3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке

Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3
---	---

Соотношение количества экспертов в зависимости от количества экзаменуемых и количества рабочих мест.

Таблица 3. Расчет количества экспертов исходя из количества рабочих мест и участников.

Количество постов-рабочих мест на экзаменационной площадке	Количество участников <u>на одно пост-рабочее</u> место на одной экзаменационной площадке (по умолчанию 1 участник)	Максимальное количество участников в одной экзаменационной группе одной экзаменационной площадки	Количество экспертов на одну экзаменационную группу одной экзаменационной площадки
1	2	3	4
1	1	1	3
2	1	2	3
3	1	3	3
4	1	4	3
5	1	5	3
6	1	6	3
7	1	7	3
8	1	8	3
9	1	9	3
10	1	10	3
11	1	11	3
12	1	12	3
13	1	13	4
14	1	14	4
15	1	15	4
16	1	16	4
17	1	17	4
18	1	18	4
19	1	19	4
20	1	20	4
21	1	21	5
22	1	22	5
23	1	23	5
24	1	24	5
25	1	25	5

4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

По результатам выполнения заданий демонстрационного экзамена может быть применена схема перевода баллов из стобалльной шкалы в оценки по пятибалльной шкале.

Таблица 4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

Оценка	«2»	«3»	«4»	«5»
1	2	3	4	5
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00% - 19,99%	20,00% - 39,99%	40,00% - 69,99%	70,00% - 100,00%

5. Список оборудования и материалов, запрещенных на площадке (при наличии)

Таблица 5. Список оборудования и материалов, запрещенных на площадке, (при наличии)

№ п/п	Наименование запрещенного оборудования
1	2
1	Личный мобильный телефон (смартфон)
2	Наушники с передачей аудио (проводные, беспроводные)
3	Личный ноутбук
4	Личный планшет
5	Личная клавиатура
6	Личная компьютерная мышь

6. Детальная информация о распределении баллов и формате оценки.

Таблица 6. Обобщенная оценочная ведомость.

№ п/п	Модуль задания, где проверяется критерий	Критерий	Длительность модуля	Разделы WSSS	Судейские баллы	Объективные баллы	Общие баллы
1	2	3	4	5	6	7	8
1	А: Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	1:30:00	2	0,00	14,00	14,00
2	Е: Технологии защиты узла и агентского мониторинга	Технологии защиты узла и агентского мониторинга	2:00:00	6	0,00	18,00	18,00
3	С: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	2:00:00	4	0,00	18,00	18,00
4	Ф: Предотвращение инцидентов и управление событиями информационной безопасности	Предотвращение инцидентов и управление событиями информационной безопасности	0:30:00	7	0,00	4,00	4,00
Итого	-	-	6:00:00	-	0,00	54,00	54,00

7. Примерный план работы Центра проведения демонстрационного экзамена¹.

Таблица 7. Примерный план работы Центра проведения демонстрационного экзамена.

День (выберете из выпадающего списка)	Начало мероприяти я (укажите в формате ЧЧ:ММ)	Окончание мероприяти я (укажите в формате ЧЧ:ММ)	Длительность мероприятия (расчет производится автоматическ и)	Мероприятие	Действия экспертной группы при распределенном формате ДЭ (Заполняется при выборе распределенного формата ДЭ)	Действия экзаменуемых при распределенно м формате ДЭ (Заполняется при выборе распределенног о формата ДЭ)	Действия экспертной группы при дистанционном формате ДЭ (Заполняется при выборе дистанционного формата ДЭ)	Действия экзаменуемых при дистанционно м формате ДЭ (Заполняется при выборе дистанционног о формата ДЭ)
1	2	3	4	5	6	7	8	9
Подготовительны й день (С-1)	9:00:00	9:15:00	0:15:00	Получение главным экспертом задания демонстрационног о экзамена	—	—	—	—
Подготовительны й день (С-1)	9:15:00	10:00:00	0:45:00	Проверка готовности проведения демонстрационног о экзамена, заполнение Акта о готовности площадки	Проверка подключения к площадке, сверка участников	—	Проверка подключения к площадке, сверка участников	—

¹ Если планируется проведение демонстрационного экзамена для двух и более экзаменационных групп (ЭГ) из одной учебной группы одновременно на одной площадке, то это также должно быть отражено в плане. Примерный план рекомендуется составить таким образом, чтобы продолжительность работы экспертов на площадке не превышала нормы, установленные действующим законодательством. В случае необходимости превышения установленной продолжительности по объективным причинам, требуется согласование с экспертами, задействованными для работы на соответствующей площадке.

Подготовительный день (С-1)	10:00:00	10:15:00	0:15:00	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение протоколов	Заполнение протоколов онлайн	—	Заполнение протоколов онлайн	—
Подготовительный день (С-1)	10:15:00	10:30:00	0:15:00	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Проверка подключения к площадке	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Проверка подключения к площадке
Подготовительный день (С-1)	10:30:00	10:45:00	0:15:00	Регистрация участников демонстрационного экзамена	Контроль за регистрацией	Регистрация с помощью веб-камеры (мобильного телефона или иного устройства)	Контроль за регистрацией	Регистрация с помощью веб-камеры (мобильного телефона или иного устройства)
Подготовительный день (С-1)	10:45:00	11:15:00	0:30:00	Инструктаж участников по охране труда и технике безопасности, сбор подписей в протоколах	Контроль за протоколами	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Контроль за протоколами	Инструктаж по ОТиТБ, заполнение протоколов онлайн

Подготовительный день (С-1)	11:15:00	13:00:00	1:45:00	Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение протоколов	Контроль за протоколами, жеребьевкой	Жеребьевка, проверка подключения к рабочим местам, заполнение протоколов онлайн	Контроль за протоколами, жеребьевкой	Жеребьевка, проверка подключения к рабочим местам, заполнение протоколов онлайн
Подготовительный день (С-1)	13:00:00	16:00:00	3:00:00	Подготовка и/или проверка работоспособности и площадки в соответствии с заданием	Проверка работоспособности и площадки, помощь ГЭ (при необходимости), Завершение дня	Завершение дня	Проверка работоспособности и площадки, помощь ГЭ (при необходимости), Завершение дня	Завершение дня
День 1	8:45:00	9:00:00	0:15:00	Ознакомление с заданием и правилами	Подключение к площадке и системе ВКС, контроль за подключением участников	Подключение к площадке и системе ВКС, получение задания, ознакомление	Подключение к площадке и системе ВКС, контроль за подключением участников	Подключение к площадке и системе ВКС, получение задания, ознакомление
День 1	9:00:00	9:15:00	0:15:00	Брифинг		Ознакомление с заданием, вопросы		Ознакомление с заданием, вопросы
День 1	9:15:00	10:45:00	1:30:00	Выполнение модуля А	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 1	10:45:00	11:00:00	0:15:00	Перерыв, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв

День 1	11:00:00	13:00:00	2:00:00	Выполнение модуля Е	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 1	13:00:00	13:45:00	0:45:00	Обед, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 1	13:45:00	15:45:00	2:00:00	Выполнение модуля С	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 1	15:45:00	16:00:00	0:15:00	Перерыв, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 1	16:00:00	17:30:00	1:30:00	Выполнение модуля F	Контроль за участниками и выполнением работ	Выполнение работ, завершение работы	Контроль за участниками и выполнением работ	Выполнение работ, завершение работы
День 1	17:30:00	19:30:00	2:00:00	Работа экспертов, заполнение форм и оценочных ведомостей	Оценка работ с помощью средств удаленного управления (подключения к площадке), проставление баллов	—	Оценка работ с помощью средств удаленного управления (подключения к площадке), проставление баллов	—

День 1	19:30:00	20:30:00	1:00:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение протоколов	Внесение баллов в CIS, подписание протокола с использованием ЭП или сканирования (фото) протокола	—	Внесение баллов в CIS, подписание протокола с использованием ЭП или сканирования (фото) протокола	—
--------	----------	----------	---------	--	---	---	---	---

8. Необходимые приложения

Приложение 2. Соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами.

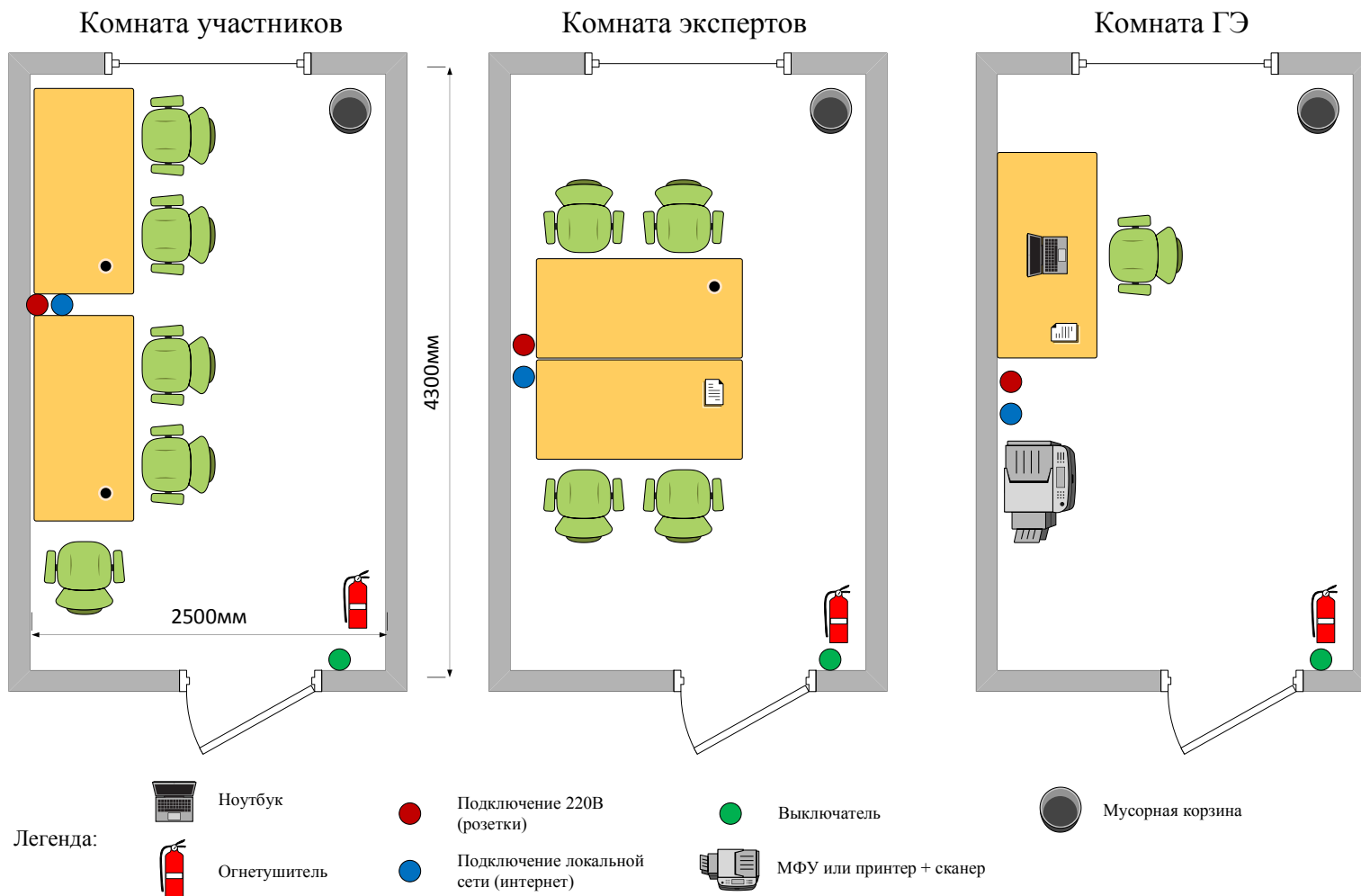
Приложение 5. План застройки площадки для проведения демонстрационного экзамена.

Приложение 6. Инфраструктурный(-ые) лист(-ы).

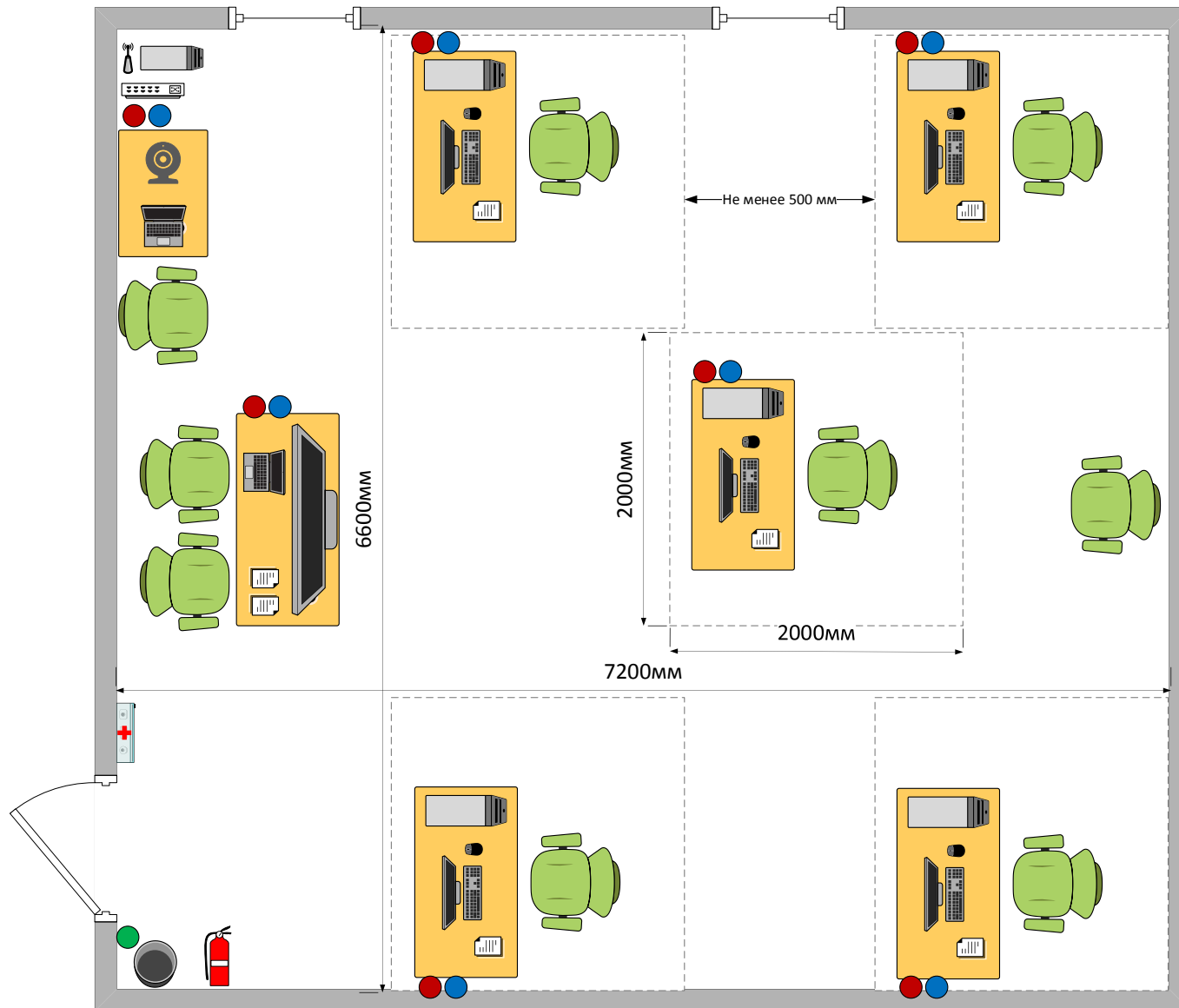
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный)

Формат проведения ДЭ: очный / распределенный

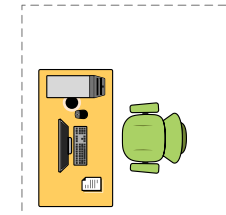
Общая площадь площадки: 80 м²



Площадка проведения экзамена



Легенда



Рабочее место (2×2 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, USB-накопитель, набор ПО



Ноутбук



Аптечка



Огнетушитель



ТВ/проектор (таймер)



Камера (трансляция)



Сетевая инфраструктура (сервер, коммутатор/маршрутизатор, точка доступа), может быть в серверной



Подключение 220В (розетки)



Подключение локальной сети (интернет)



Выключатель



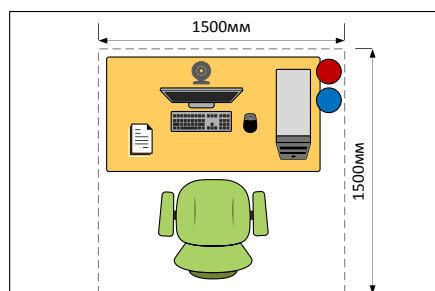
Мусорная корзина

План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (дистанционный)

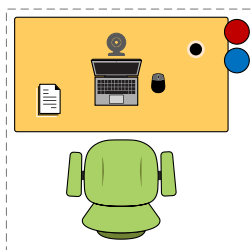
Формат проведения ДЭ: дистанционный

Общая площадь площадки: 2,25 м² (и более, на 1 участника/эксперта)

Рабочее место участника

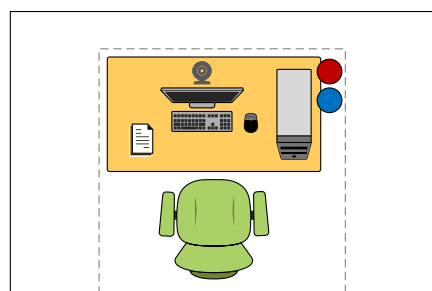


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

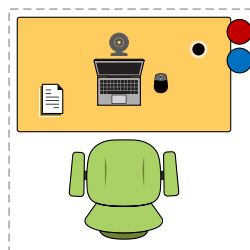


Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

Рабочее место эксперта

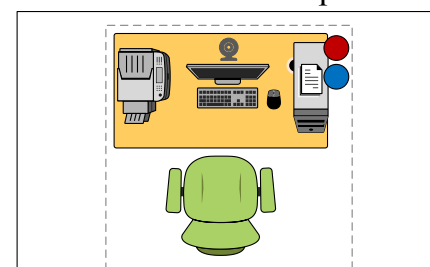


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

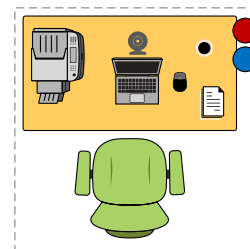


Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

Рабочее место главного эксперта

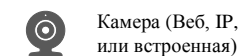


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, МФУ (принтер и сканер) или принтер + камера или смартфон (для «сканирования») набор ПО, доступ к Интернет (кабель или беспроводной)



Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, МФУ (принтер и сканер) или принтер + камера или смартфон (для «сканирования»), набор ПО, доступ к Интернет (кабель или беспроводной)

Легенда:



Камера (Веб, IP, или встроенная)



Подключение 220В (розетки)



Подключение локальной сети (интернет) или WiFi



МФУ или принтер + сканер, или принтер + камера/ смартфон/ планшет прочее с камерой

Образец задания

Образец задания для демонстрационного экзамена по комплексу оценочной документации.

Описание задания

В компании «Демо Лаб» возникла необходимость внедрения DLP системы для лучшей защиты разработок и предотвращения утечек прочей информации. Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием. Основными каналами потенциальной утечки данных являются электронная почта и различные интернет-ресурсы, если не указано иное.

Политики трафика могут быть проверены вручную или с помощью генератора событий, предоставляемым по запросу.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены (кроме адреса DNS сервера на машинах).

Перед экзаменом должны быть подготовлены следующие виртуальные машины для работы (рекомендуется сделать нулевой Snapshot для быстрой подготовки к другим потокам), сеть настроена в режиме NAT (сеть NAT) или Bridge с DHCP, с доступом в интернет, но без доступа к машинам других участников экзамена:

- AD и DNS сервер (контроллер домена), 1,5ГБ ОЗУ и выше, 2 ядра, статическая адресация с доступом в интернет,
- DLP сервер установлен (но не настроен), активирована лицензия, 6ГБ ОЗУ и выше, 2 ядра,
- Виртуальная машина для установки сервера агентского мониторинга, 2ГБ ОЗУ и выше, 2 ядра,
- Виртуальные машины «нарушителей» (2 шт), 1,5ГБ ОЗУ и выше, 2 ядра.

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов (demo.lab, должен быть развернут из эталонного, получить эталон можно по запросу).

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными. При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и документацией на компьютерах.

Все дистрибутивы должны находиться в каталоге, указанном в карточке задания. Все логины, пароли, сетевые настройки и прочее, относящееся к инфраструктуре площадки, должно быть указано в карточке задания.

При создании снимков экрана необходимо делать либо полный снимок экрана, либо целого окна.

Описание модуля А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Задание 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “Test” в корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

Внутри созданного подразделения “Test” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: user1, пароль: ххХХ1234, права пользователя домена

Логин: user2, пароль: ххХХ1234, права пользователя домена

Логин: admin1, пароль: ххХХ1234, права администратора домена

Логин: user3, пароль: ххХХ1234, права пользователя домена

Логин: user4, пароль: ххХХ1234, права пользователя домена

Задание 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен.

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя user4.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена user3 с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» на рабочем столе компьютера.

Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя admin1 (важно). После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “Test” на домене.

Установить базу данных PostgreSQL или функциональный аналог с паролем суперпользователя ххХХ1234.

Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токenu, но можно сделать это и после

установки. При установке настроить локального пользователя консоли управления: officer с паролем xxXX1234

Синхронизировать каталог пользователей и компьютеров с Active Directory или функциональным аналогом.

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя admin1, установить полный доступ к системе, установить все области видимости.

Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.

Задание 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину 1 в домен, после перезагрузки войти в систему от ранее созданного пользователя user1.

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя user2.

После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение “Test” на домене.

Установить агент мониторинга:

На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга.

На машину 2 с помощью групповых политик домена.

Необходимо создавать отдельные объекты групповых политик на каждое задание и делать снимки экрана для подтверждения создания и выполнения политик.

Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания

Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов.

Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга с настройками по умолчанию.

Необходимо создать общий каталог Test в корне диска сервера и установить права доступа на запись и чтение для всех пользователей домена.

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. Для работы подсистемы может потребоваться редактирование конфигурационных файлов (для устранения предупреждения).

Задание 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих некий термин, установить уровень угрозы для всех событий, добавить тег.

Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя 1 с установленным агентом.

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа, настроив конструктор выборки вручную.

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задание 7: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должны удовлетворять общепринятым на сегодня стандартам и требованиям, параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать:

1. корневой root-сертификат (ca)
2. серверный (server) сертификат
3. по желанию допускается использование пользовательского и промежуточного сертификата

Поля сертификата заполняются по вариантам заданий.

После генерации сертификатов необходимо установить серверный сертификат на веб-сервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена для использования на всех

компьютерах в сети для доверенного подключения к веб-консоли DLP-системы уровня сети.

Итоговый результат должен включать:

Дерево из 2-3 сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе. Содержимое команд по генерации ключей и сертификатов в текстовом файле на рабочем столе с комментариями.

Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).

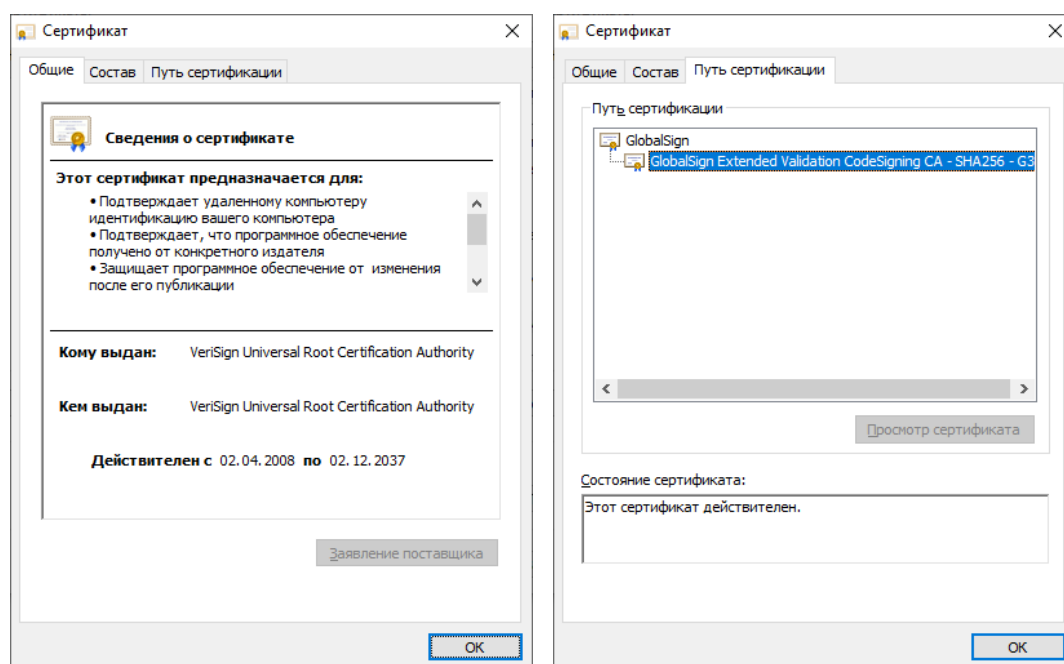


Рис1. Пример скриншотов задания

Описание модуля Е: Технологии защиты узла и агентский мониторинг

Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании). Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна. Выполнение отдельных

заданий необходимо подтвердить скриншотом (это всегда указывается отдельно).

Задание 1

Необходимо создать 2 новых группы компьютеров: «Test1» и «Test2», а также создать 2 новых политики: «Test1» и «Test2». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 необходимо перенести в Test1, а компьютер 2 — в Test2.

Зафиксировать выполнение скриншотом.

Задание 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на другую машину для удаленного доступа к серверу агентского мониторинга.

Следующие правила создаются в политике «Test1».

Правило 1

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 3

Ограничить доступ к определенным облачным хранилищам (по вариантам).

Проверить работоспособность и зафиксировать выполнение

Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Правило 5

Необходимо запретить запись файлов на определенные носители информации, при этом оставить возможность считывания информации.

Проверить работоспособность и зафиксировать выполнение

Правило 6

С учетом ранее созданной блокировки необходимо разрешить использование доверенного носителя информации.

Проверить работоспособность и зафиксировать выполнение

Правило 7

Полностью запретить использование определенного устройства для пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 8

С учетом ранее выполненного запрета необходимо предоставить временный доступ для определенного устройства не определенное время для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Следующие правила создаются в политике «Test2».

Правило 9

Необходимо поставить на контроль буфер обмена в блокноте и notepad++. Проверить занесение нескольких событий в WEB-консоль.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 10

Необходимо запретить использовать терминальные сессии для пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 11

Необходимо установить контроль за компьютером потенциального нарушителя путем создания снимков экрана каждые 60 секунд или при смене окна.

Проверить работоспособность и зафиксировать выполнение

Правило 12

Запретить передачу файлов определенного типа на съемные носители информации или в сетевое расположение.

Проверить работоспособность и зафиксировать выполнение

Групповые политики домена

Групповые применяются только на компьютер 2, должны быть созданы в домене. Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например запрет запуска).

Групповая политика 1

Настроить политику паролей и блокировки: Максимальный срок действия пароля, Минимальная длина пароля, Сложность пароля, Блокировка учетной записи при неверном вводе пароля.

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Запретить запуск приложений по списку (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

Запретить использование элементов системы стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельно менять параметры системы (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

Настроить дополнительные параметры системы, которые должны применяться для пользователя или компьютера (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Описание модуля С: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям. Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием. После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Для некоторых политик могут понадобиться дополнительные файлы, расположение которых можно узнать из карточки задания или у экспертов.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). Скриншоты необходимо сохранить в папке «Модуль 3».

Скриншоты необходимо называть в соответствии с номером задания и типом задания (Например Политика 2, Задание 1–1 и т. д.)

Задания на разработку политик можно выполнять в любом порядке.

Наиболее сложные политики находятся в конце.

При разработке политик стоит учитывать, что все политики трафика могут передаваться как через веб-сообщения, так и через почтовые сообщения. В случае, если данный пункт не соблюден, то проверка заданий может быть невозможной.

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации.

Список тегов для политик:

Политика 1, Политика 2, Политика 3, ...

Задание 1

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты.

Задание 2

Создайте локальную группу пользователей и добавьте в нее пользователей.

Задание 3

Создать список веб-ресурсов. Добавить в список следующие сайты: Site.ru, domain.com, ...

Задание 4

Для работы системы необходимо настроить периметр компании: Почтовый домен, список веб ресурсов, группа персон, исключить из перехвата.

Политика 1

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела (по вариантам) отправлять документы, содержащие информацию о паспортных данных за пределы компании. Отдел (по вариантам) может отправлять файлы без ограничений.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 1

Политика 2

Для контроля за движением документов необходимо вести наблюдение за передачей шаблона документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах определенного уровня.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 2

Политика 3

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в

социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика.

Вердикт: заблокировать

Уровень нарушения: низкий

Тег: Политика 3

Политика 4

Необходимо отслеживать документы, содержащие печать компании всем сотрудникам, кроме отдела (по вариантам) и определенного сотрудника. Они могут обмениваться документами внутри и за пределами компании без контроля.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 4

Политика 5

В последнее время возникла необходимость обработки текстовых данных, а также сканов и фото кредитных карт. Необходимо отслеживать передачу всех возможных данных кредитных карт (в том числе сканов) за пределы компании.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 5

Политика 6

Сотрудники заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из определенного отдела, для остальных контролировать не нужно.

Критичными данными в выгрузке являются определенные поля и в 1 документе присутствует более 1 строчки. Для настройки используйте файл примера.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 6

Политика 7

Некая компания попросила обеспечить защиту от утечки важных данных. Необходимо создать политику на контроль правила передачи содержащие слова «один», «два», «три» в 1 сообщении или документе одновременно. Если в документе встречается только по 1 слову из перечисленных — политика срабатывать не должна.

Правило должно срабатывать на сообщения, которые отправляются за пределы компании всеми пользователями, кроме определенного отдела, который может отсылать информацию свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 7

Политика 8

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании за пределы компании, запрещая любую внешнюю передачу документов в пустых и заполненных бланках.

Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 8

Политика 9

Пользователи стали часто обмениваться ссылками и файлами, в связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов, например формата.mp4 и ссылок определенного формата (содержит уникальную последовательность, например urlname). Ложных срабатываний быть не должно.

Вердикт: Заблокировать

Уровень нарушения: средний

Тег: Политика 9

Политика 10

Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость

отследить утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты.

Важно, чтобы в одном сообщении содержалось минимум 2 адреса (т. к. в противном случае будут детектироваться все почтовые сообщения)!

Возможные домены первого уровня: ru, org и прочие. Детектирование только частей адресов (например @mail.ru) недопустимо.

Вердикт: разрешить

Уровень нарушения: высокий

Тег: Политика 10

Политика 11

В связи с разгильдяйством сотрудников, передающих свои пароли коллегам с помощью почты и сообщений, необходимо предотвратить передачу любых стандартизированных паролей для информационной системы в открытом виде любыми отправителями и получателями как внутри, так и за пределы компании.

Стоит учесть, что пароли могут передаваться любым указанным способом: социальные сети и прочие ресурсы (в браузере), мессенджеры, почта, флешки. Необходимо также контролировать наличие паролей в сетевых каталогах.

Стоит учесть, что отдел так как генерацией паролей занимается отдел ИТ, то пользователи отдела могут рассылать пароли пользователям совершенно свободно, но только внутри компании.

Стандартизированные форматы паролей (кириллица):

6 букв – 1 знак !?#\$%^/_& – 2-4 цифры – 4 буквы – 2-3 знака !?#\$%^/_&
(например, ПаРоль#67рКнЕ!?)

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 11

Политика 12

Необходимо контролировать передачу определенных типов файлов только за пределы компании.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 12

Описание модуля F: Предотвращение инцидентов и управление событиями информационной безопасности

Задание 1: Контроль доступа

Необходимо создать пользователя DLP системы с определенными правами просмотра и редактирования.

Задание 2: Сводки

Создайте новые вкладки сводки в разделе «Сводка»

Задание 3: Виджеты

Создайте в сводке 4 виджета:

1. Выборка по событиям за период
2. Выборка по политикам с технологиями за период
3. Статистика за период
4. По нарушителям за период

Задание 4

Необходимо создать виджет отображающий события определенного типа (с определенного устройства и т. п.) за период.

Зафиксировать скриншотом конструктора выборки.

Задание 5

Необходимо создать виджет отображающий события определенного уровня (определенных политик и т. п.) за период.

Необходимые приложения

Приложение 1: Карточка настроек сети и оборудования (docx)

Приложение 2: Шаблоны документов для задания (zip)

3. Комплект оценочной документации паспорт КОД 1.2– 2022

Паспорт комплекта оценочной документации

1. Описание

Комплект оценочной документации (КОД) разработан в целях организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия.

В данном разделе указаны основные характеристики КОД и должны использоваться при планировании, проведении и оценки результатов демонстрационного экзамена образовательными организациями, ЦПДЭ и Агентством.

Таблица 1. Паспорт комплекта оценочной документации (КОД)

№ п/п	Наименование	Информация о разработанном КОД
1	2	3
1	Номер компетенции	F7
2	Название компетенции	Корпоративная защита от внутренних угроз информационной безопасности
3	КОД является однодневным или двухдневным:	Однодневный
4	Номер КОД	КОД 1.2
4.1	Год(ы) действия КОД	2022 (1 год)
5	Уровень ДЭ	ФГОС СПО
6	Общее максимально возможное количество баллов задания по всем критериям оценки	30,00
7	Длительность выполнения экзаменационного задания данного КОД	5:30:00
8	КОД разработан на основе	ФНЧ Молодые профессионалы 2021
9	КОД подходит для проведения демонстрационного экзамена в качестве процедуры Независимой оценки квалификации (НОК)	НЕТ
10	Вид аттестации, для которой подходит данный КОД	ГИА, Промежуточная
11	Формат проведения ДЭ	X
11.1	КОД разработан для проведения ДЭ в очном формате, (участники и эксперты находятся в ЦПДЭ)	Да
11.2	КОД разработан для проведения ДЭ в дистанционном формате, (участники и эксперты работают удаленно)	Да
11.3	КОД разработан для проведения ДЭ в распределенном формате, (детализация в п.11.3.1)	Да
11.3.1	Формат работы в распределенном формате	Участники находятся в ЦПДЭ, эксперты работают удаленно
12	Форма участия (индивидуальная, парная, групповая)	Индивидуальная

12.1	Количество человек в группе, (т.е. задание ДЭ выполняется индивидуально или в группе/ команде из нескольких экзаменуемых)	1,00
12.2	Организация работы при невозможности разбить экзаменуемых на указанное в п. 12.1 количество человек в группе	
13	Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3,00
16	Автоматизированная оценка результатов заданий	Автоматизация неприменима
16.1	Что автоматизировано: заполняется при выборе вариантов в п.16: возможна частичная или полная автоматизация	

2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта

Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта, (WorldSkills Standards Specification WSSS), проверяемый в рамках комплекта оценочной документации, (Таблица 2).

Таблица 2. WSSS

Номер раздела WSSS	Наименование раздела WSSS	Содержание раздела WSSS: Специалист должен знать	Важность раздела WSSS (%)
1	2	3	4
2	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	Специалист должен знать и понимать:Сетевое окружение; Сетевые протоколы; Знать методы выявления и построения путей движения информации в организации;Подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия; Типы сетевых устройств;Разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз; Процесс выбора подходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем; Важность следования инструкциям и последствия, цену пренебрежения ими; Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы; Этапы установки системы корпоративной защиты от внутренних угроз;Знать отличия различных версий систем корпоративной защиты от внутренних угроз;Знать какие СУБД поддерживаются системой;Знать назначение различных компонент версий систем корпоративной защиты от внутренних угроз;Знать технологии программной и аппаратной виртуализации;Знать особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation;Цель документирования процессов обновления и установки.Важность спокойного и сфокусированного подхода к решению проблемы; Значимость систем ИТ-безопасности и зависимость пользователей и организаций от их доступности; Популярные аппаратные и программные ошибки; Знать разделы системы корпоративной безопасности, которые обычно использует системный администратор;Аналитический и диагностический подходы к решению проблем; Границы собственных знаний, навыков и полномочий; Ситуации, требующие вмешательства службы поддержки; Стандартное время решения наиболее популярных проблем.Специалист должен уметь:Интерпретировать пользовательские запросы и требования с точки зрения корпоративных	14,00

		<p>требований; Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении; Настраивать сетевые устройства; Администрирование автоматизированных технических средства управления и контроля информации и информационных потоков; Навыки системного администрирования в операционных системах Windows, Windows Server, Linux (Red Hat Enterprise Linux, CentOS и др.); Навыки системного администрирования в защищенных операционных системах (AstraLinux и др.); Настройка в операционных системах прав доступа в соответствие с ролевой и/или мандатной моделью; Настройка средств виртуализации под операционными системам; Конфигурирование операционных систем для правильного и защищенного использования средств безопасности, в т.ч. системы корпоративной защиты от внутренних угроз.; Установка серверной части системы корпоративной защиты от внутренних угроз; Установка СУБД различного вида; Установка агентской части системы корпоративной защиты от внутренних угроз; Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом; Использовать дополнительные утилиты если это необходимо; Уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки; Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае необходимости; Уметь сконфигурировать систему, чтобы она получала теневые копии; Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах; Демонстрировать уверенность и упорство в решении проблем; Быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы, точно описывать проблему и документировать её решение; Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей; Выбирать и принимать диагностирующее ПО и инструменты для поиска неисправностей;</p>	
5	Технологии защиты и анализа сетевого трафика	<p>Специалист должен знать и понимать: Организационно-технические и правовые основы использования электронного документооборота в информационных системах; Структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей; Нормативно-правовые документы, требования законодательства и регулирующих органов РФ в области электронной подписи, удостоверяющих центров, СКЗИ, МЭ; Классы защищенности и уровни доверия СЗИ; Технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений; Ключевые компоненты VPN-</p>	16,00

		<p>сетей; Особенности VPN-сети и механизмы их управления; Современные криптографические алгоритмы. Криптопровайдеры, криптографические интерфейсы и библиотеки; Архитектура, основные компоненты PKI их функции и взаимодействие; Назначение и роль доверенного удостоверяющего центра в системе ключевой инфраструктуры организации; Жизненный цикл ключей и сертификатов; Электронный сертификат ключей ЭП. Формирование, подписание и использование сертификатов; Защита видео и конференций приложений; Назначение и основные сценарии применения IDS-технологий; Архитектуру и особенности внедрения IDS-технологий; Распространённые вектора атак и уязвимости современных корпоративных информационных систем. Специалист должен уметь: Осуществлять развёртывание и администрирование VPN-сети (добавление, удаление, изменение объектов сети, настройка параметров работы, контроль работоспособности и др.). Обновление ПО, установленного на узлах защищенной сети. Работать и удостоверяющей и ключевой информацией. Формирование и управление ключевой структурой сети. Издание и управление сертификатами пользователей. Настраивать защиту сегментов IP-сетей, координация работы узлов защищенной сети. Защиты трафика, передаваемого по открытым каналам связи; Осуществлять защиту оконечных рабочих мест; Контроль пользовательских приложений; Реализовывать межсетевое взаимодействие и туннелирование; Компрометация рабочих мест; Обеспечение межсетевого экранирования и криптографической защиты информации; Производить установку, настройку, развёртывание удостоверяющих центров инфраструктуры открытых ключей включая подсистемы регистрации пользователей, создания ключей ЭП, издания сертификатов ключей проверки ЭП, поддержания инфраструктуры ключей проверки ЭП. Конфигурировать ПО для электронного документооборота в VPN-системах; Защита систем, обеспечивающих поддержку процессинформационного взаимодействия; Выполнять настройку и проверку работоспособности; Проводить детектирование атак (потенциальных угроз) в ручном, автоматизированном и автоматическом режиме; Проводить правильную классификацию уровня угрозы инцидента; Использовать базы контентной фильтрации; Использовать дополнительные модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса;</p>	
--	--	--	--

*Таблица соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами доступна в Приложении

3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке

Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3
---	---

Соотношение количества экспертов в зависимости от количества экзаменуемых и количества рабочих мест.

Таблица 3. Расчет количества экспертов исходя из количества рабочих мест и участников.

Количество постов-рабочих мест на экзаменационной площадке	Количество участников <u>на одно пост-рабочее</u> место на одной экзаменационной площадке (по умолчанию 1 участник)	Максимальное количество участников в одной экзаменационной группе одной экзаменационной площадки	Количество экспертов на одну экзаменационную группу одной экзаменационной площадки
1	2	3	4
1	1	1	3
2	1	2	3
3	1	3	3
4	1	4	3
5	1	5	3
6	1	6	3
7	1	7	3
8	1	8	3
9	1	9	3
10	1	10	3
11	1	11	3
12	1	12	3
13	1	13	4
14	1	14	4
15	1	15	4
16	1	16	4
17	1	17	4
18	1	18	4
19	1	19	4
20	1	20	4
21	1	21	5
22	1	22	5
23	1	23	5
24	1	24	5
25	1	25	5

4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

По результатам выполнения заданий демонстрационного экзамена может быть применена схема перевода баллов из стобалльной шкалы в оценки по пятибалльной шкале.

Таблица 4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

Оценка	«2»	«3»	«4»	«5»
1	2	3	4	5
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00% - 19,99%	20,00% - 39,99%	40,00% - 69,99%	70,00% - 100,00%

5. Список оборудования и материалов, запрещенных на площадке (при наличии)

Таблица 5. Список оборудования и материалов, запрещенных на площадке, (при наличии)

№ п/п	Наименование запрещенного оборудования
1	2
1	Личный мобильный телефон (смартфон)
2	Наушники с передачей аудио (проводные, беспроводные)
3	Личный ноутбук
4	Личный планшет
5	Личная клавиатура
6	Личная компьютерная мышь

6. Детальная информация о распределении баллов и формате оценки.

Таблица 6. Обобщенная оценочная ведомость.

№ п/п	Модуль задания, где проверяется критерий	Критерий	Длительность модуля	Разделы WSSS	Судейские баллы	Объективные баллы	Общие баллы
1	2	3	4	5	6	7	8
1	А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	3:00:00	2,5	0,00	16,00	16,00
2	Д: Технологии защиты и анализа сетевого трафика	Технологии защиты и анализа сетевого трафика	2:30:00	2,5	0,00	14,00	14,00
Итого	-	-	5:30:00	-	0,00	30,00	30,00

7. Примерный план работы Центра проведения демонстрационного экзамена².

Таблица 7. Примерный план работы Центра проведения демонстрационного экзамена.

День (выберете из выпадающего списка)	Начало мероприяти я (укажите в формате ЧЧ:ММ)	Окончание мероприяти я (укажите в формате ЧЧ:ММ)	Длительность мероприятия (расчет производится автоматически)	Мероприятие	Действия экспертной группы при распределенном формате ДЭ (Заполняется при выборе распределенного формата ДЭ)	Действия экзаменуемых при распределенно м формате ДЭ (Заполняется при выборе распределенно о формата ДЭ)	Действия экспертной группы при дистанционном формате ДЭ (Заполняется при выборе дистанционного формата ДЭ)	Действия экзаменуемых при дистанционно м формате ДЭ (Заполняется при выборе дистанционно о формата ДЭ)
1	2	3	4	5	6	7	8	9
Подготовительны й день (С-1)	09:00:00	09:15:00	0:15:00	Получение главным экспертом задания демонстрационн о экзамена	—	—	—	—
Подготовительны й день (С-1)	09:15:00	10:00:00	0:45:00	Проверка готовности проведения демонстрационн о экзамена, заполнение Акта о готовности площадки	Проверка подключения к площадке, сверка участников	—	Проверка подключения к площадке, сверка участников	—
Подготовительны й день (С-1)	10:00:00	10:15:00	0:15:00	Распределение обязанностей по	Заполнение протоколов	—	Заполнение протоколов	—

² Если планируется проведение демонстрационного экзамена для двух и более экзаменационных групп (ЭГ) из одной учебной группы одновременно на одной площадке, то это также должно быть отражено в плане. Примерный план рекомендуется составить таким образом, чтобы продолжительность работы экспертов на площадке не превышала нормы, установленные действующим законодательством. В случае необходимости превышения установленной продолжительности по объективным причинам, требуется согласование с экспертами, задействованными для работы на соответствующей площадке.

				проведению экзамена между членами Экспертной группы, заполнение протоколов	онлайн		онлайн	
Подготовительный день (С-1)	10:15:00	10:30:00	0:15:00	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Проверка подключения к площадке	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Проверка подключения к площадке
Подготовительный день (С-1)	10:30:00	10:45:00	0:15:00	Регистрация участников демонстрационного экзамена	Контроль за регистрацией	Регистрация с помощью веб-камеры (мобильного телефона или иного устройства)	Контроль за регистрацией	Регистрация с помощью веб-камеры (мобильного телефона или иного устройства)
Подготовительный день (С-1)	10:45:00	11:15:00	0:30:00	Инструктаж участников по охране труда и технике безопасности, сбор подписей в протоколах	Контроль за протоколами	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Контроль за протоколами	Инструктаж по ОТиТБ, заполнение протоколов онлайн
Подготовительный день (С-1)	11:15:00	13:00:00	1:45:00	Распределение рабочих мест и ознакомление с рабочими местами,	Контроль за протоколами, жеребьевкой	Жеребьевка, проверка подключения к рабочим местам, заполнение	Контроль за протоколами, жеребьевкой	Жеребьевка, проверка подключения к рабочим местам,

				оборудованием, графиком работы, иной документацией и заполнение протоколов		протоколов онлайн		заполнение протоколов онлайн
Подготовительный день (С-1)	13:00:00	16:00:00	3:00:00	Подготовка и/или проверка работоспособности и площадки в соответствии с заданием	Проверка работоспособности и площадки, помощь ГЭ (при необходимости), Завершение дня	Завершение дня	Проверка работоспособности и площадки, помощь ГЭ (при необходимости), Завершение дня	Завершение дня
День 1	08:45:00	09:00:00	0:15:00	Ознакомление с заданием и правилами	Подключение к площадке и системе ВКС, контроль за подключением участников	Подключение к площадке и системе ВКС, получение задания, ознакомление	Подключение к площадке и системе ВКС, контроль за подключением участников	Подключение к площадке и системе ВКС, получение задания, ознакомление
День 1	09:00:00	09:15:00	0:15:00	Брифинг		Ознакомление с заданием, вопросы		Ознакомление с заданием, вопросы
День 1	09:15:00	10:45:00	1:30:00	Выполнение модуля А	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 1	10:45:00	11:00:00	0:15:00	Перерыв, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 1	11:00:00	12:30:00	1:30:00	Выполнение модуля А	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ

День 1	12:30:00	13:15:00	0:45:00	Обед, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 1	13:15:00	14:30:00	1:15:00	Выполнение модуля D	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 1	14:30:00	14:45:00	0:15:00	Перерыв, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 1	14:45:00	16:00:00	1:15:00	Выполнение модуля D	Контроль за участниками и выполнением работ	Выполнение работ, завершение работы	Контроль за участниками и выполнением работ	Выполнение работ, завершение работы
День 1	16:00:00	18:00:00	2:00:00	Работа экспертов, заполнение форм и оценочных ведомостей	Оценка работ с помощью средств удаленного управления (подключения к площадке), проставление баллов	—	Оценка работ с помощью средств удаленного управления (подключения к площадке), проставление баллов	—
День 1	18:00:00	19:00:00	1:00:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение протоколов	Внесение баллов в CIS, подписание протокола с использованием ЭП или сканирования (фото) протокола	—	Внесение баллов в CIS, подписание протокола с использованием ЭП или сканирования (фото) протокола	—

8. Необходимые приложения

Приложение 2. Соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами.

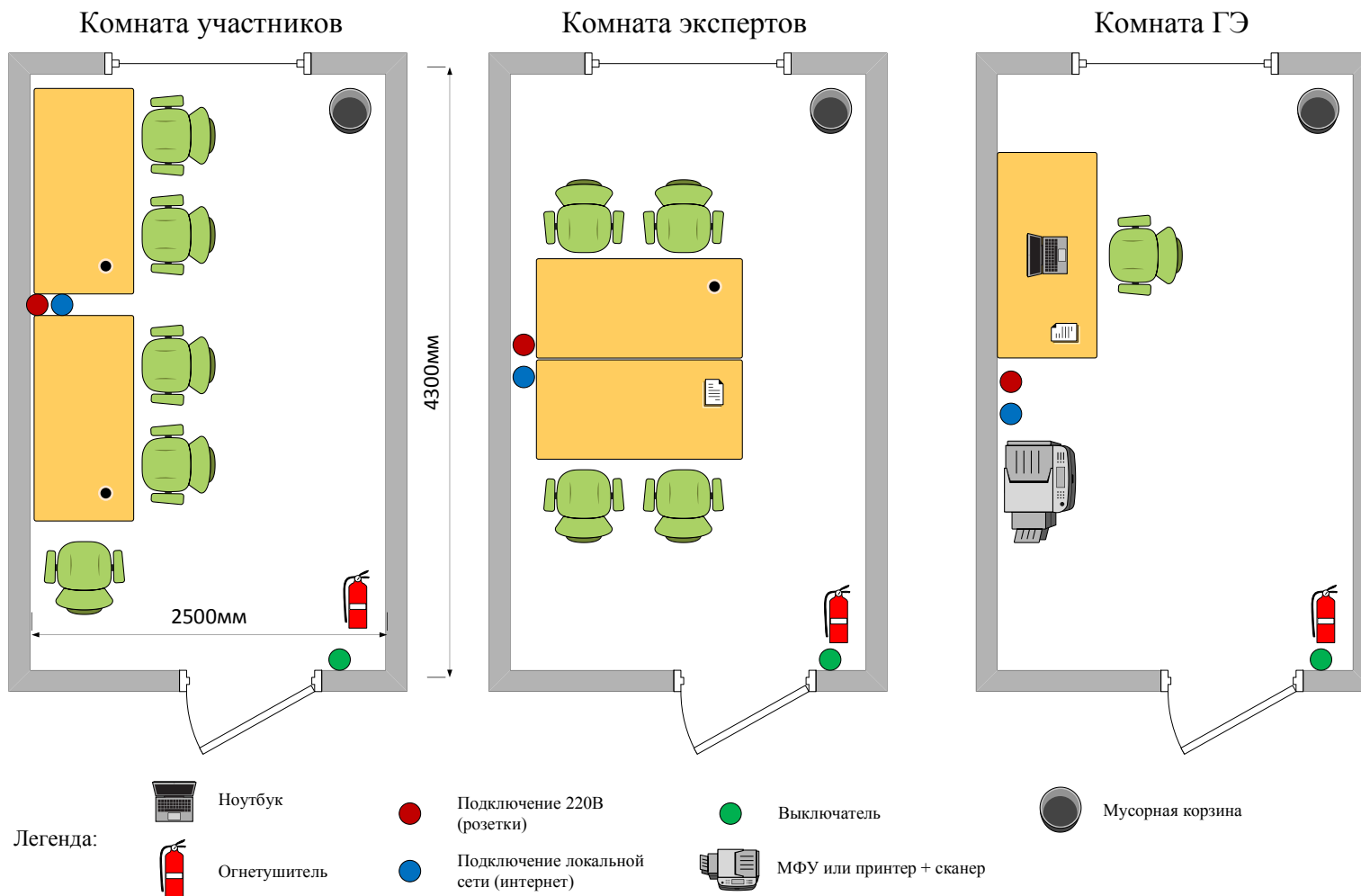
Приложение 5. План застройки площадки для проведения демонстрационного экзамена.

Приложение 6. Инфраструктурный(-ые) лист(-ы).

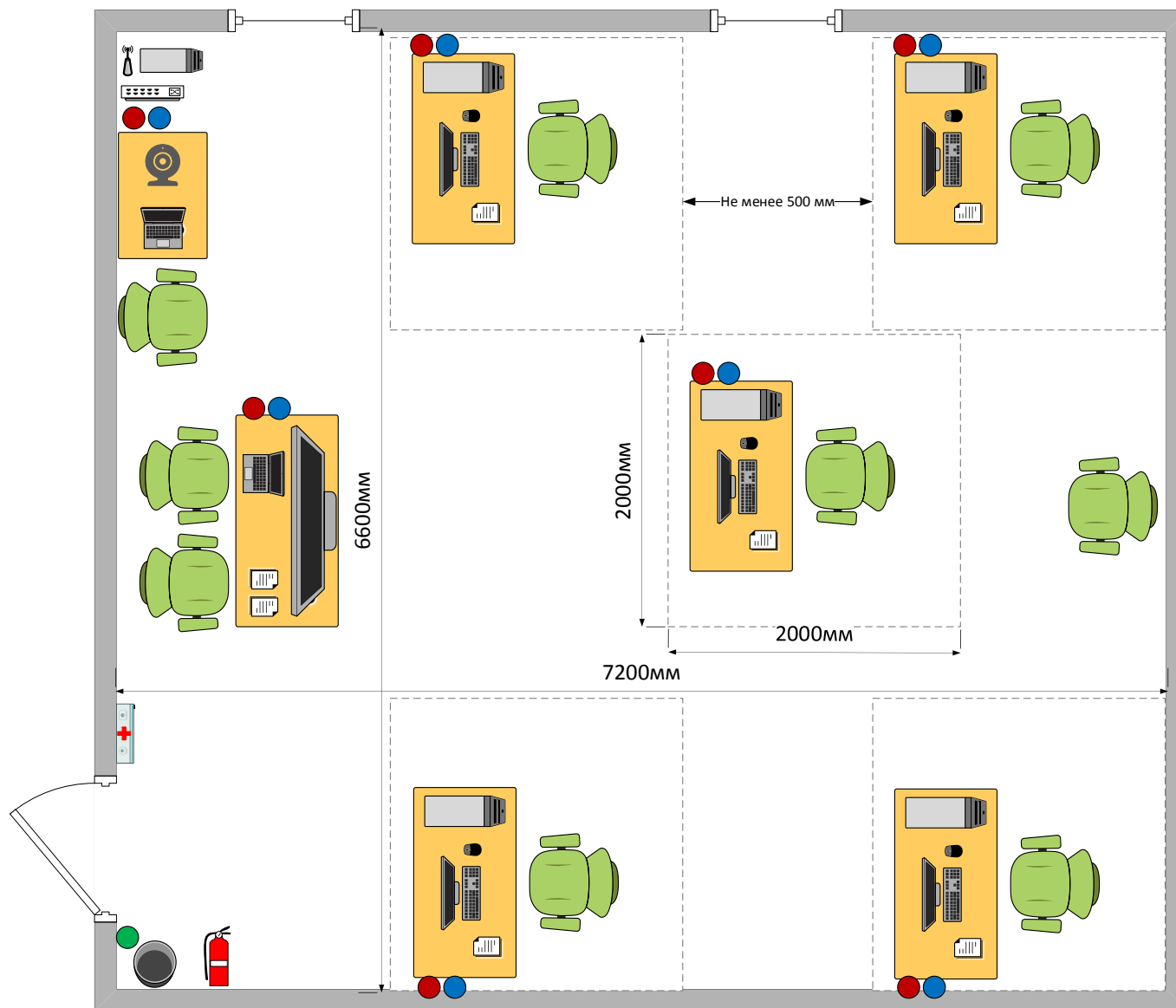
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный)

Формат проведения ДЭ: очный / распределенный

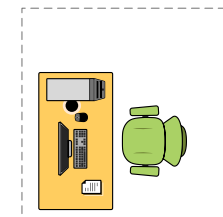
Общая площадь площадки: 80 м²



Площадка проведения экзамена



Легенда



Рабочее место (2×2 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, USB-накопитель, набор ПО



Ноутбук



Аптечка



Огнетушитель



ТВ/проектор
(таймер)



Камера (трансляция)



Сетевая инфраструктура (сервер, коммутатор/маршрутизатор, точка доступа), может быть в серверной



Подключение 220В (розетки)



Подключение локальной сети (интернет)



Выключатель



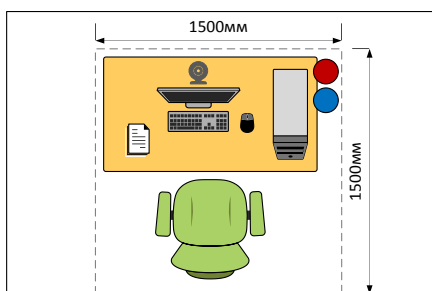
Мусорная корзина

План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (дистанционный)

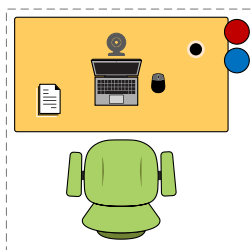
Формат проведения ДЭ: дистанционный

Общая площадь площадки: 2,25 м² (и более, на 1 участника/эксперта)

Рабочее место участника

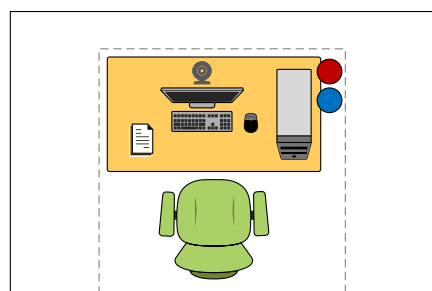


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

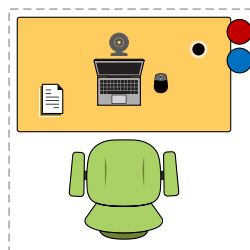


Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

Рабочее место эксперта

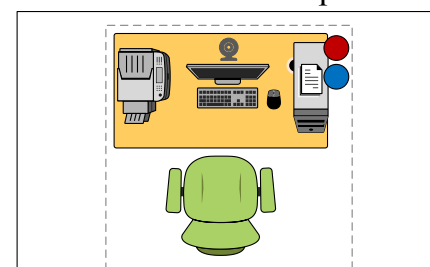


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

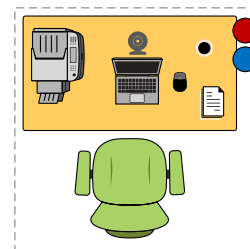


Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

Рабочее место главного эксперта

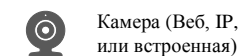


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, МФУ (принтер и сканер) или принтер + камера или смартфон (для «сканирования») набор ПО, доступ к Интернет (кабель или беспроводной)



Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, МФУ (принтер и сканер) или принтер + камера или смартфон (для «сканирования»), набор ПО, доступ к Интернет (кабель или беспроводной)

Легенда:



Камера (Веб, IP, или встроенная)



Подключение 220В (розетки)



Подключение локальной сети (интернет) или WiFi



МФУ или принтер + сканер, или принтер + камера/ смартфон/ планшет прочее с камерой

Образец задания

С помощью технологии виртуальных машин для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах (Главный офис — виртуальные машины, Офис филиал — виртуальные машины).

При выполнении заданий необходимо ключевые настройки подтверждать скриншотами. Скриншоты необходимо сохранить на рабочем столе в папке «Модуль (номер)». Формат названия скриншотов: ITCS-1-2-1.jpg (задание 1.2, скриншот 1). Можно добавить комментарий (ITCS-1-2-1-Coordinator).

В ходе выполнения данного задания нужно установить основное ПО на рабочие станции будущей защищенной сети.

Доступ на все машины указан в дополнительной карточке задания

В случае изменения каких-либо логинов или паролей необходимо отобразить это в отчете.

Настройки сетевого окружения

Для правильной работы сети надо создать или убедиться в наличии 4 сетей:

- Host only или внутренняя сеть адаптер для сети центрального офиса
- Host only или внутренняя сеть адаптер для сети филиала
- Host only или внутренняя сеть адаптер для сети межсетевого взаимодействия
- Host only адаптер, NAT или Bridge для виртуального «Интернета» (в соответствии с инфраструктурой площадки, для связи всех координаторов между собой)

В случае иных настроек инфраструктуры экзаменационной площадки необходимо изменить данные сведения в задании!

IP адреса защищенных сетей

- Центральный офис «Сеть 1 ЦО»: 1.2.3.0/28
- Офис филиал «Сеть 1 Филиал»: 2.3.4.0/27
- Офис сеть 2 «Сеть 2 Офис»: 5.6.7.0/26
- «Интернет» для всех координаторов: 8.9.10.0/24

Адреса выбираются самостоятельно из указанного диапазона.

Необходимо записать все IP адреса, логины и пароли в текстовый файл VPN.txt на рабочем столе компьютера.

В связи с особенностями работы системы на серверных версиях необходимо устанавливать компоненты системы вручную (например, БД, сервер ЦУС, клиент ЦУС) используя пакеты MSI в подпапках дистрибутивов.

Описание модуля А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Задание 1.1. Развертывание ПК Administrator в качестве центра сертификации

Установить базу данных на VM Net1-DB (незащищенный узел)

Установить и настроить рабочее место администратора Certification Authority (на базе виртуальной машины Net1-Admin (ЦО)): Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД.

Установить клиент ЦУС на VM Net1-DB (незащищенный узел)

Если были произведены изменения паролей, IP-адресов и так далее, необходимо отразить это в отчете.

Задание 1.2. Установка ПО VPN Coordinator и ПО VPN Client для Certification Authority

1. установить ПО Client, рабочее место администратора;
2. установить и инициализировать ПО Coordinator HW-VA;

Задание 1.3. Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины

1. установить ПО Client.
2. установить ПО Publication Service.
3. установить ПО Registration Point.
4. установить ПО CA Informing.

Задание 1.4. Установка ПО Coordinator и ПО Client для организации сети филиала

1. установить и инициализировать ПО Coordinator HW-VA.
2. установить ПО Client, рабочее место пользователя.

Необходимо зафиксировать процесс установки скриншотами форм + сделать скриншот директории, в которую установлено ПО, и скриншот первого запуска приложения.

Задание 1.5. Развертывание удостоверяющего центра в составе сети

Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

Схема сети, которую требуется создать, приведена далее.

IP адреса сетей перечислены в начале задания (по названию сетей).

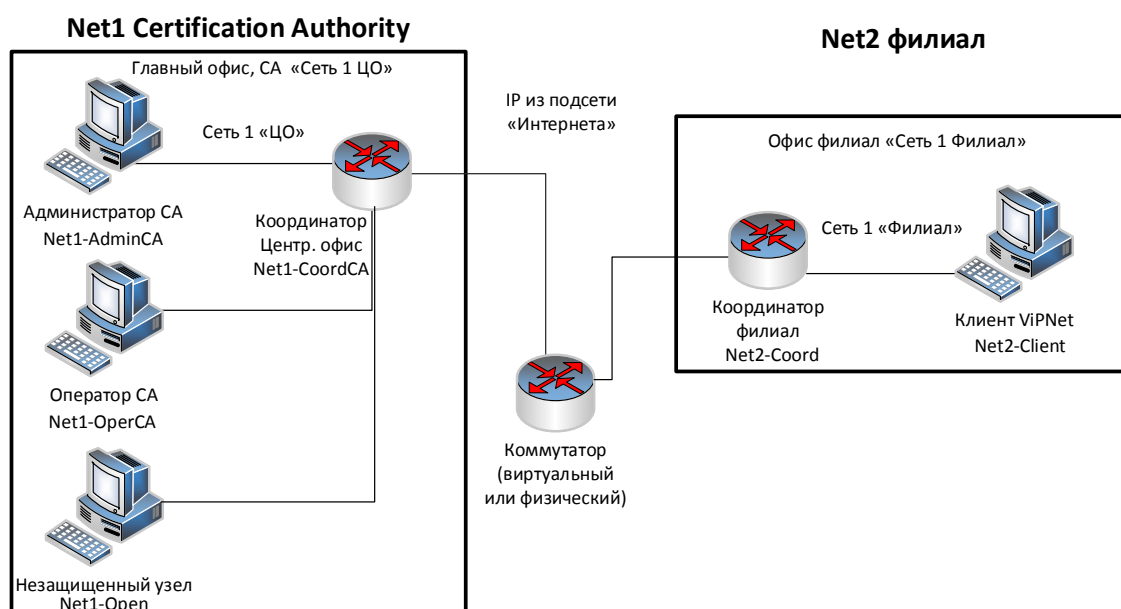


Рисунок 1 Схема защищенной сети

В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).

Таблица 1 Узлы защищенной сети если УКЦ и ЦУС на одной машине.

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1-AdminCA (ЦО)	Главный администратор (VM)	Administrator (ЦУС клиент и сервер + УКЦ), Client, CA Informing	ОС пользовательская или серверная	AdminCA
Net1-CoordCA (ЦО)	Координатор Центр Офис (VM)	Coordinator	Координатор HW-VA	CoordinatorCA
Net1-OperCA (ЦО)	Оператор УЦ (VM)	Client, Publication Service, Registration Point	ОС пользовательская или серверная	OperCA
Net2-Coord (Филиал)	Координатор Филиал (VM)	Coordinator	Координатор HW-VA	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал (VM)	Client	ОС пользовательская или серверная	User

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	Coordinator Office	Admin	OperCA	Coordinator Subsidiary	User
CoordinatorOffice	×	*	*	*	
Admin	*	×	*		*
OperCA	*	*	×	*	
CoordinatorSub	*		*	×	*
User		*		*	×

Задание 1.6. Создание структуры защищенной сети

ЦУС. Необходимо создать в ЦУС структуру защищенной сети в соответствии с заданной схемой (выгрузить отчет в HTML). Создать пользователей узлов, настроить полномочия пользователей и их связи в соответствии со схемой.

УКЦ. Провести инициализацию УКЦ, сохранить контейнер ключей администратора в общей папке (создать подпапку Задание 1.6), поменять тип паролей для пользователей («собственный»). Задать пароли пользователей и сохранить в текстовый файл. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить на жесткий диск). Создать группы узлов для центрального офиса (удостоверяющего центра) и филиала, настроить пароль администратора группы сетевых узлов для каждой из групп (проверить, что пароль работает).

На всех узлах сети корректно настроить или проверить корректность настройки сетевых интерфейсов в соответствии со схемой, проверить доступность соседних узлов.

Разнести DST файлы по АРМ, провести первичную инициализацию узлов защищенной сети (координаторов и клиентов), проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов.

Задание 1.7. Настройка работы удостоверяющего центра в аккредитованном режиме

Необходимо перевести УКЦ в режим аккредитованного удостоверяющего центра, настроить параметры издания квалифицированных сертификатов, указав:

- сведения о средствах УЦ,
- средство электронной подписи издателя
- средства удостоверяющего центра
- сертификат на средство электронной подписи издателя
- сертификат на средство удостоверяющего центра
- класс защищенности, которому соответствуют программные средства УЦ,
- место хранения контейнеров ключа ЭП и ключа защиты УКЦ

После перевода УКЦ в аккредитованный режим необходимо выпустить:

- Корневой квалифицированный сертификат.
- Квалифицированную электронную подпись для пользователя
- Квалифицированную электронную подпись для пользователя

При формировании сертификатов необходимо заполнить следующие поля:

- Имя: <Имя пользователя или узла>
- Электронная почта
- Город

- Область
- Организация
- Подразделение
- Почтовый индекс

Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети. Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации (Publication Service).

Реализовать автоматическую публикацию сертификатов.

Посредством Центра Регистрации (Registration Point):

1. зарегистрировать пользователя;
2. отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос;
3. отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос.

Посредством Сервиса Информирования (CA Informing):

4. настроить способ выдачи уведомлений;
5. сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов

Задание 1.8. Модификация структуры защищенной сети

Перед началом выполнения сделать HTML выгрузку структуры сети и сделать скриншот ЦУС окна с пользователями.

Модификация структуры сети:

1. добавить новый сетевой узел и пользователя за координатором (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем. На указанных узлах проверить появление нового узла;
2. Добавить пользователя на узле Филиал (Net2-Client филиала 2), связать его со всеми пользователями группы узлов центральный офис. Для указанных пользователей проверить появление новой связи;
3. отправить письмо по Деловой почте пользователю.
4. отправить текстовое сообщение пользователю

Необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:

- скриншоты деловой почты на отправителе и получателе (при отправке письма);
- скриншоты текстового сообщения на отправителе и получателе;
- скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы.

Кроме того, необходимо сохранить файл HTML с обновленной структурой защищенной сети, выгруженный из ЦУС.

Описание модуля D: Технологии защиты и анализа сетевого трафика

Задание 2.1. Компрометация узла защищенной сети

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя, т. к. в случае неудачной компрометации структура сети может нарушиться.

Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС:

1. скомпрометировать ключи пользователя на узле,
2. произвести смену ключей пользователя и сетевых узлов,
3. отправить обновления и произвести процедуру смены ключа пользователя,
4. проверить работу защищенной сети после обновления отправив сообщение от пользователя.

Восстановление взаимодействия с помощью ручной установки DST засчитано не будет.

Необходимо зафиксировать процесс настройки скриншотами или иным указанным способом:

- компрометация пользователя.
- смена ключей пользователя и сетевых узлов.
- процедура смены ключа на клиенте с использованием резервного набора ключей.
- скриншот экрана «защищенная сеть» в Monitor на узле Пользователь_2 Филиал + результат проверки доступности узлов.

Кроме того, нужно сохранить архив директории, в которой расположен резервный набор ключей на рабочем столе компьютера (после смены ключей).

Задание 2.2. Межсетевое взаимодействие защищённых сетей (со связями «все со всеми»)

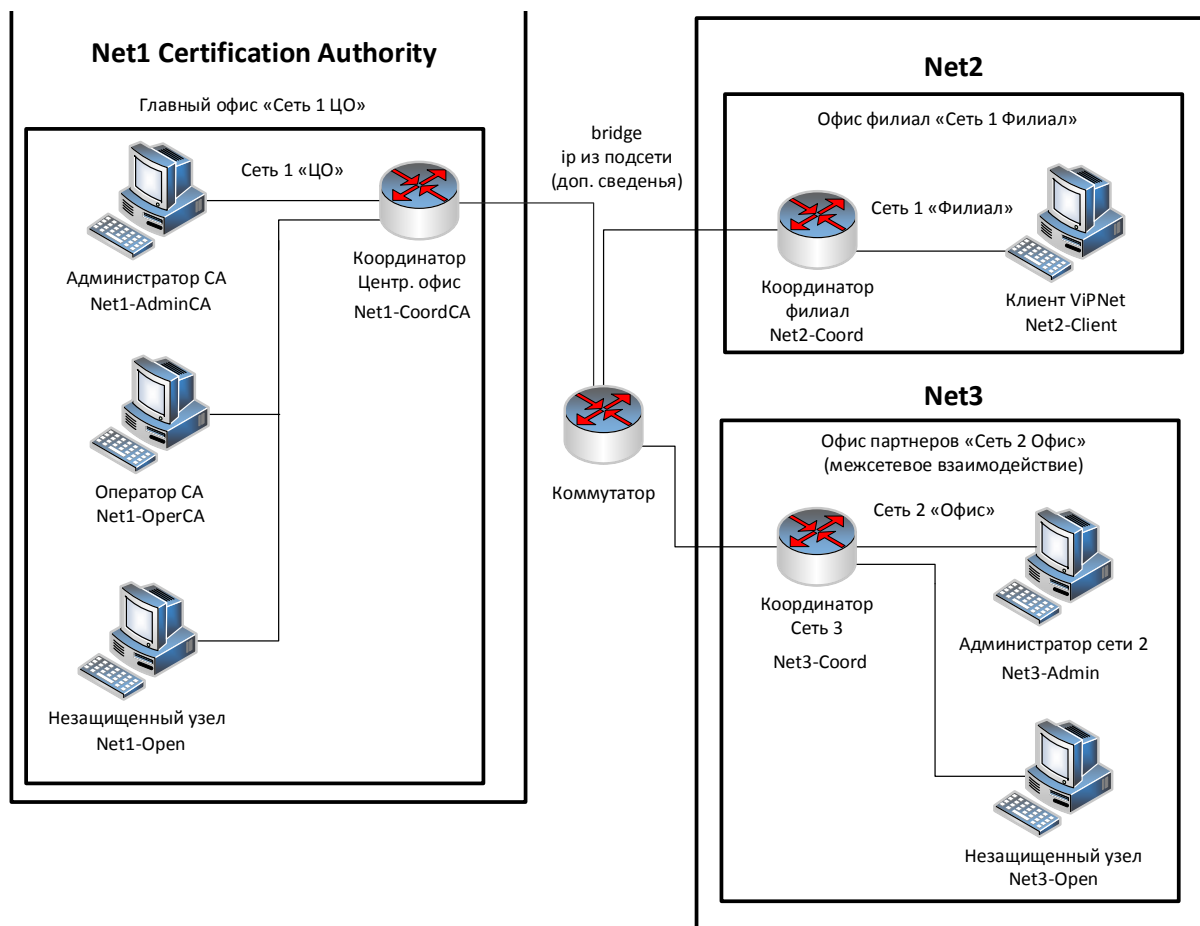


Рисунок 2 Схема межсетевого взаимодействия

Развернуть на Net3-Admin (Сеть 3 межсеть) на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети:

Рабочее место администратора (БД, ЦУС, УКЦ, Client)

- 1 координатор (HW-VA или координатор Linux),
- 1 узел Admin,
- Установите координатор.

Установить и настроить необходимое ПО

Настроить межсетевое взаимодействие между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.

Проверить взаимодействие узлов, отправив сообщение деловой почтой.

Задание 2.3. Туннелирование в рамках межсетевого взаимодействия

Подключить незащищенную машину в сети 3.

Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по зашифрованному каналу.

Проверить доступность незащищённых машин друг другу любым другим протоколом; проанализировать журналы IP-пакетов на координаторах.

Скриншоты:

- Настройка максимального количества туннелей на координаторах
- Скриншоты прохождения ICMP пакетов (ping) и любого другого трафика с незащищенного узла
- Скриншоты журнала IP-пакетов координатора с установленным фильтром «Туннелирование» для проверки прохождения ICMP-пакетов и любого другого трафика с помощью туннелирования

Необходимые приложения

Приложение 1. Карточка настроек сети и оборудования (docx)

4. Комплект оценочной документации паспорт КОД 1.3–2022

Паспорт комплекта оценочной документации

1. Описание

Комплект оценочной документации (КОД) разработан в целях организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия.

В данном разделе указаны основные характеристики КОД и должны использоваться при планировании, проведении и оценки результатов демонстрационного экзамена образовательными организациями, ЦПДЭ и Агентством.

Таблица 1. Паспорт комплекта оценочной документации (КОД)

№ п/п	Наименование	Информация о разработанном КОД
1	2	3
1	Номер компетенции	F7
2	Название компетенции	Корпоративная защита от внутренних угроз информационной безопасности
3	КОД является однодневным или двухдневным:	Однодневный
4	Номер КОД	КОД 1.3
4.1	Год(ы) действия КОД	2022 (1 год)
5	Уровень ДЭ	ФГОС СПО
6	Общее максимально возможное количество баллов задания по всем критериям оценки	31,00
7	Длительность выполнения экзаменационного задания данного КОД	3:30:00
8	КОД разработан на основе	ФНЧ Молодые профессионалы 2021
9	КОД подходит для проведения демонстрационного экзамена в качестве процедуры Независимой оценки квалификации (НОК)	НЕТ
10	Вид аттестации, для которой подходит данный КОД	Промежуточная
11	Формат проведения ДЭ	X
11.1	КОД разработан для проведения ДЭ в очном формате, (участники и эксперты находятся в ЦПДЭ)	Да
11.2	КОД разработан для проведения ДЭ в дистанционном формате, (участники и эксперты работают удаленно)	Да
11.3	КОД разработан для проведения ДЭ в распределенном формате, (детализация в п.11.3.1)	Да
11.3.1	Формат работы в распределенном формате	Участники находятся в ЦПДЭ, эксперты работают удаленно
12	Форма участия (индивидуальная, парная, групповая)	Индивидуальная

12.1	Количество человек в группе, (т.е. задание ДЭ выполняется индивидуально или в группе/ команде из нескольких экзаменуемых)	1,00
12.2	Организация работы при невозможности разбить экзаменуемых на указанное в п. 12.1 количество человек в группе	
13	Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3,00
16	Автоматизированная оценка результатов заданий	Частичная автоматизация
16.1	Что автоматизировано: заполняется при выборе вариантов в п.16: возможна частичная или полная автоматизация	Модуль 3 (в зависимости от возможностей площадки)

2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта

Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта, (WorldSkills Standards Specification WSSS), проверяемый в рамках комплекта оценочной документации, (Таблица 2).

Таблица 2. WSSS

Номер раздела WSSS	Наименование раздела WSSS	Содержание раздела WSSS: Специалист должен знать	Важность раздела WSSS (%)
1	2	3	4

2	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	<p>Специалист должен знать и понимать:</p> <p>Сетевое окружение;</p> <p>Сетевые протоколы;</p> <p>Знать методы выявления и построения путей движения информации в организации;</p> <p>Подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;</p> <p>Типы сетевых устройств;</p> <p>Разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз;</p> <p>Процесс выбора подходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем;</p> <p>Важность следования инструкциям и последствия, цену пренебрежения ими;</p> <p>Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы;</p> <p>Этапы установки системы корпоративной защиты от внутренних угроз;</p> <p>Знать отличия различных версий систем корпоративной защиты от внутренних угроз;</p> <p>Знать какие СУБД поддерживаются системой;</p> <p>Знать назначение различных компонент версий систем корпоративной защиты от внутренних угроз;</p> <p>Знать технологии программной и аппаратной виртуализации;</p> <p>Знать особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation;</p> <p>Цель документирования процессов обновления и установки.</p> <p>Важность спокойного и сфокусированного подхода к решению проблемы;</p> <p>Значимость систем ИТ-безопасности и зависимость пользователей и организаций от их доступности;</p> <p>Популярные аппаратные и программные ошибки;</p> <p>Знать разделы системы корпоративной безопасности, которые обычно использует системный администратор;</p> <p>Аналитический и диагностический подходы к решению проблем;</p> <p>Границы собственных знаний, навыков и полномочий;</p> <p>Ситуации, требующие вмешательства службы поддержки;</p> <p>Стандартное время решения наиболее популярных проблем.</p> <p>Специалист должен уметь:</p> <p>Интерпретировать пользовательские запросы и требования с точки зрения корпоративных требований;</p>	5,00
---	---	--	------

		<p>Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении; Настраивать сетевые устройства; Администрирование автоматизированных технических средства управления и контроля информации и информационных потоков; Навыки системного администрирования в операционных системах Windows, Windows Server, Linux (Red Hat Enterprise Linux, CentOS и др.); Навыки системного администрирования в защищенных операционных системах (AstraLinux и др.); Настройка в операционных системах прав доступа в соответствие с ролевой и/или мандатной моделью; Настройка средств виртуализации под операционными системам; Конфигурирование операционных систем для правильного и защищенного использования средств безопасности, в т.ч. системы корпоративной защиты от внутренних угроз.:</p> <p>Установка серверной части системы корпоративной защиты от внутренних угроз; Установка СУБД различного вида; Установка агентской части системы корпоративной защиты от внутренних угроз; Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом; Использовать дополнительные утилиты если это необходимо; Уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки; Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае необходимости; Уметь сконфигурировать систему, чтобы она получала теневые копии; Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах; Демонстрировать уверенность и упорство в решении проблем; Быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы, точно описывать проблему и документировать её решение; Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей; Выбирать и принимать диагностирующее ПО и инструменты для поиска неисправностей;</p>	
--	--	---	--

4	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	<p>Специалист должен знать и понимать:</p> <p>Технологии работы с политиками информационной безопасности;</p> <p>Создание новых политик, модификация существующих;</p> <p>Общие принципы при работе интерфейсом системы защиты корпоративной информации;</p> <p>Объекты защиты, персоны;</p> <p>Ключевые технологии анализа трафика;</p> <p>Типовые протоколы и потоки данных в корпоративной среде, такими как: корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4) веб-почта;</p> <p>Интернет-ресурсы: сайты, блоги, форумы и т.д. (протоколы HTTP, HTTPS); социальные сети;</p> <p>интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP;</p> <p>принтеры: печать файлов на локальных и сетевых принтерах;</p> <p>любые съемные носители и устройства;</p> <p>Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек;</p> <p>Типы угроз информационной безопасности, типы инцидентов,</p> <p>Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;</p> <p>Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации;</p> <p>Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;</p> <p>Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации;</p> <p>Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки;</p> <p>Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе;</p> <p>Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов;</p> <p>Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации;</p> <p>Специалист должен уметь:</p> <p>Создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты;</p>	10,00
---	---	--	-------

		<p>Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты;</p> <p>Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии;</p> <p>Работа со сводками, виджетами, сводками;</p> <p>Работа с персонами;</p> <p>Работа с объектами защиты;</p> <p>Провести имитацию процесса утечки конфиденциальной информации в системе;</p> <p>Создать непротиворечивые политики, соответствующие нормативной базе и законодательству;</p> <p>Задokumentировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации.</p> <p>Работа с категориями и терминами;</p> <p>Использование регулярных выражений;</p> <p>Использование морфологического поиска;</p> <p>Работа с графическими объектами;</p> <p>Работа с выгрузками и баз данных;</p> <p>Работа с печатями и бланками;</p> <p>Работа с файловыми типами;</p> <p>Эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;</p>	
6	Технологии защиты узла и агентского мониторинга	<p>Специалист должен знать и понимать:</p> <p>Функции агентского мониторинга;</p> <p>Общие настройки системы агентского мониторинга;</p> <p>Соединение с LDAP-сервером и синхронизация с Active Directory;</p> <p>Политики агентского мониторинга, особенности их настройки;</p> <p>Особенности настроек событий агентского мониторинга;</p> <p>Механизмы диагностики агента, подходы к защите агента.</p> <p>Знать возможности и ограничения современных российских и зарубежных операционных систем в рамках решения задач защиты информации</p> <p>Знать архитектуру операционных систем</p> <p>Знать инструментарий по работа с современными операционными системами, команды, ПО, утилиты</p> <p>Специалист должен уметь:</p> <p>Установка и настройка агентского мониторинга;</p> <p>Создание политик защиты на агентах;</p> <p>Работа в консоли управления агентом;</p> <p>Фильтрация событий;</p> <p>Настройка совместных событий агентского и сетевого мониторинга;</p>	12,00

		<p>Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата. Производить настройку сервисов и компонент операционной системы для достижения целей защиты Разделять компоненты операционной системы по уровням доверия, сокращая поверхность атаки для злоумышленника Применять механизмы ролевого и мандатного доступа и контроля целостности Реализовывать ограниченную программную среду для пользователя Знать особенности безопасной работы и загрузки операционных систем на различных аппаратных платформах</p>	
7	<p>Предотвращение инцидентов и управление событиями информационной безопасности</p>	<p>Специалист должен знать и понимать: Назначение, роль, возможности систем IDS/IPS для задачи защиты организации от угроз информационной безопасности Назначение, роль, возможности систем SIEM для задачи защиты организации от угроз информационной безопасности Назначение, роль, возможности систем Threat Intelligence для задачи защиты организации от угроз информационной безопасности Специалист должен уметь: Устанавливать, настраивать системы IDS/IPS Устанавливать, настраивать системы SIEM Устанавливать, настраивать системы Threat Intelligence, генерации трафика и проверки защищенности Применять на практике системы IDS/IPS для выявления инцидентов информационной безопасности Применять на практике системы Threat Intelligence Применять на практике системы Threat Intelligence и Attack Simulation (Breach and Attack Simulation) для проверки/оценки устойчивости систем и сетей к компьютерным атакам Проводить анализ выявленных инцидентов, использовать встроенные и внешние системы подготовки отчетности</p>	4,00

*Таблица соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами доступна в Приложении

3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке

Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3
---	---

Соотношение количества экспертов в зависимости от количества экзаменуемых и количества рабочих мест.

Таблица 3. Расчет количества экспертов исходя из количества рабочих мест и участников.

Количество постов-рабочих мест на экзаменационной площадке	Количество участников <u>на одно пост-рабочее</u> место на одной экзаменационной площадке (по умолчанию 1 участник)	Максимальное количество участников в одной экзаменационной группе одной экзаменационной площадки	Количество экспертов на одну экзаменационную группу одной экзаменационной площадки
1	2	3	4
1	1	1	3
2	1	2	3
3	1	3	3
4	1	4	3
5	1	5	3
6	1	6	3
7	1	7	3
8	1	8	3
9	1	9	3
10	1	10	3
11	1	11	3
12	1	12	3
13	1	13	4
14	1	14	4
15	1	15	4
16	1	16	4
17	1	17	4
18	1	18	4
19	1	19	4
20	1	20	4
21	1	21	5
22	1	22	5
23	1	23	5
24	1	24	5
25	1	25	5

4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

По результатам выполнения заданий демонстрационного экзамена может быть применена схема перевода баллов из стобалльной шкалы в оценки по пятибалльной шкале.

Таблица 4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

Оценка	«2»	«3»	«4»	«5»
1	2	3	4	5
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00% - 19,99%	20,00% - 39,99%	40,00% - 69,99%	70,00% - 100,00%

5. Список оборудования и материалов, запрещенных на площадке (при наличии)

Таблица 5. Список оборудования и материалов, запрещенных на площадке, (при наличии)

№ п/п	Наименование запрещенного оборудования
1	2
1	Личный мобильный телефон (смартфон)
2	Наушники с передачей аудио (проводные, беспроводные)
3	Личный ноутбук
4	Личный планшет
5	Личная клавиатура
6	Личная компьютерная мышь

6. Детальная информация о распределении баллов и формате оценки.

Таблица 6. Обобщенная оценочная ведомость.

№ п/п	Модуль задания, где проверяется критерий	Критерий	Длительность модуля	Разделы WSSS	Судейские баллы	Объективные баллы	Общие баллы
1	2	3	4	5	6	7	8
1	А:Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	0:30:00	2	0,00	5,00	5,00
2	Е:Технологии защиты узла и агентского мониторинга	Технологии защиты узла и агентского мониторинга	1:30:00	6	0,00	12,00	12,00
3	С:Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	1:00:00	4	0,00	10,00	10,00
4	Ф:Предотвращение инцидентов и управление событиями информационной безопасности	Предотвращение инцидентов и управление событиями информационной безопасности	0:30:00	7	0,00	4,00	4,00
Итого	-	-	3:30:00	-	0,00	31,00	31,00

7. Примерный план работы Центра проведения демонстрационного экзамена³.

Таблица 7. Примерный план работы Центра проведения демонстрационного экзамена.

День (выберете из выпадающего списка)	Начало мероприяти я (укажите в формате ЧЧ:ММ)	Окончание мероприяти я (укажите в формате ЧЧ:ММ)	Длительность мероприятия (расчет производится автоматическ и)	Мероприятие	Действия экспертной группы при распределенном формате ДЭ (Заполняется при выборе распределенного формата ДЭ)	Действия экзаменуемых при распределенно м формате ДЭ (Заполняется при выборе распределенно о формата ДЭ)	Действия экспертной группы при дистанционном формате ДЭ (Заполняется при выборе дистанционного формата ДЭ)	Действия экзаменуемых при дистанционно м формате ДЭ (Заполняется при выборе дистанционно о формата ДЭ)
1	2	3	4	5	6	7	8	9
Подготовительны й день (С-1)	9:00:00	9:15	0:15:00	Получение главным экспертом задания демонстрационно го экзамена	—	—	—	—
Подготовительны й день (С-1)	9:15:00	10:00:00	0:45:00	Проверка готовности проведения демонстрационно го экзамена, заполнение Акта о готовности площадки	Проверка подключения к площадке, сверка участников	—	Проверка подключения к площадке, сверка участников	—

³ Если планируется проведение демонстрационного экзамена для двух и более экзаменационных групп (ЭГ) из одной учебной группы одновременно на одной площадке, то это также должно быть отражено в плане. Примерный план рекомендуется составить таким образом, чтобы продолжительность работы экспертов на площадке не превышала нормы, установленные действующим законодательством. В случае необходимости превышения установленной продолжительности по объективным причинам, требуется согласование с экспертами, задействованными для работы на соответствующей площадке.

Подготовительный день (С-1)	10:00:00	10:15:00	0:15:00	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение протоколов	Заполнение протоколов онлайн	—	Заполнение протоколов онлайн	—
Подготовительный день (С-1)	10:15:00	10:30:00	0:15:00	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Проверка подключения к площадке	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Проверка подключения к площадке
Подготовительный день (С-1)	10:30:00	10:45:00	0:15:00	Регистрация участников демонстрационного экзамена	Контроль за регистрацией	Регистрация с помощью веб-камеры (мобильного телефона или иного устройства)	Контроль за регистрацией	Регистрация с помощью веб-камеры (мобильного телефона или иного устройства)
Подготовительный день (С-1)	10:45:00	11:15:00	0:30:00	Инструктаж участников по охране труда и технике безопасности, сбор подписей в протоколах	Контроль за протоколами	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Контроль за протоколами	Инструктаж по ОТиТБ, заполнение протоколов онлайн

Подготовительный день (С-1)	11:15:00	13:00:00	1:45:00	Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение протоколов	Контроль за протоколами, жеребьевкой	Жеребьевка, проверка подключения к рабочим местам, заполнение протоколов онлайн	Контроль за протоколами, жеребьевкой	Жеребьевка, проверка подключения к рабочим местам, заполнение протоколов онлайн
Подготовительный день (С-1)	13:00:00	16:00:00	3:00:00	Подготовка и/или проверка работоспособности и площадки в соответствии с заданием	Проверка работоспособности и площадки, помощь ГЭ (при необходимости), Завершение дня	Завершение дня	Проверка работоспособности и площадки, помощь ГЭ (при необходимости), Завершение дня	Завершение дня
День 1	8:45:00	9:00:00	0:15:00	Ознакомление с заданием и правилами	Подключение к площадке и системе ВКС, контроль за подключением участников	Подключение к площадке и системе ВКС, получение задания, ознакомление	Подключение к площадке и системе ВКС, контроль за подключением участников	Подключение к площадке и системе ВКС, получение задания, ознакомление
День 1	9:00:00	9:15:00	0:15:00	Брифинг		Ознакомление с заданием, вопросы		Ознакомление с заданием, вопросы
День 1	9:15:00	9:45:00	0:30:00	Выполнение модуля А	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 1	9:45:00	11:15:00	1:30:00	Выполнение модуля Е	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ

День 1	11:15:00	11:30:00	0:15:00	Перерыв, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 1	11:30:00	12:30:00	1:00:00	Выполнение модуля С	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 1	12:30:00	13:00:00	0:30:00	Выполнение модуля F	Контроль за участниками и выполнением работ	Выполнение работ, завершение работы	Контроль за участниками и выполнением работ	Выполнение работ, завершение работы
День 1	13:00:00	14:30:00	1:30:00	Работа экспертов, заполнение форм и оценочных ведомостей	Оценка работ с помощью средств удаленного управления (подключения к площадке), проставление баллов	—	Оценка работ с помощью средств удаленного управления (подключения к площадке), проставление баллов	—
День 1	14:30:00	15:30:00	1:00:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение протоколов	Внесение баллов в CIS, подписание протокола с использованием ЭП или сканирования (фото) протокола	—	Внесение баллов в CIS, подписание протокола с использованием ЭП или сканирования (фото) протокола	—

8. Необходимые приложения

Приложение 2. Соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами.

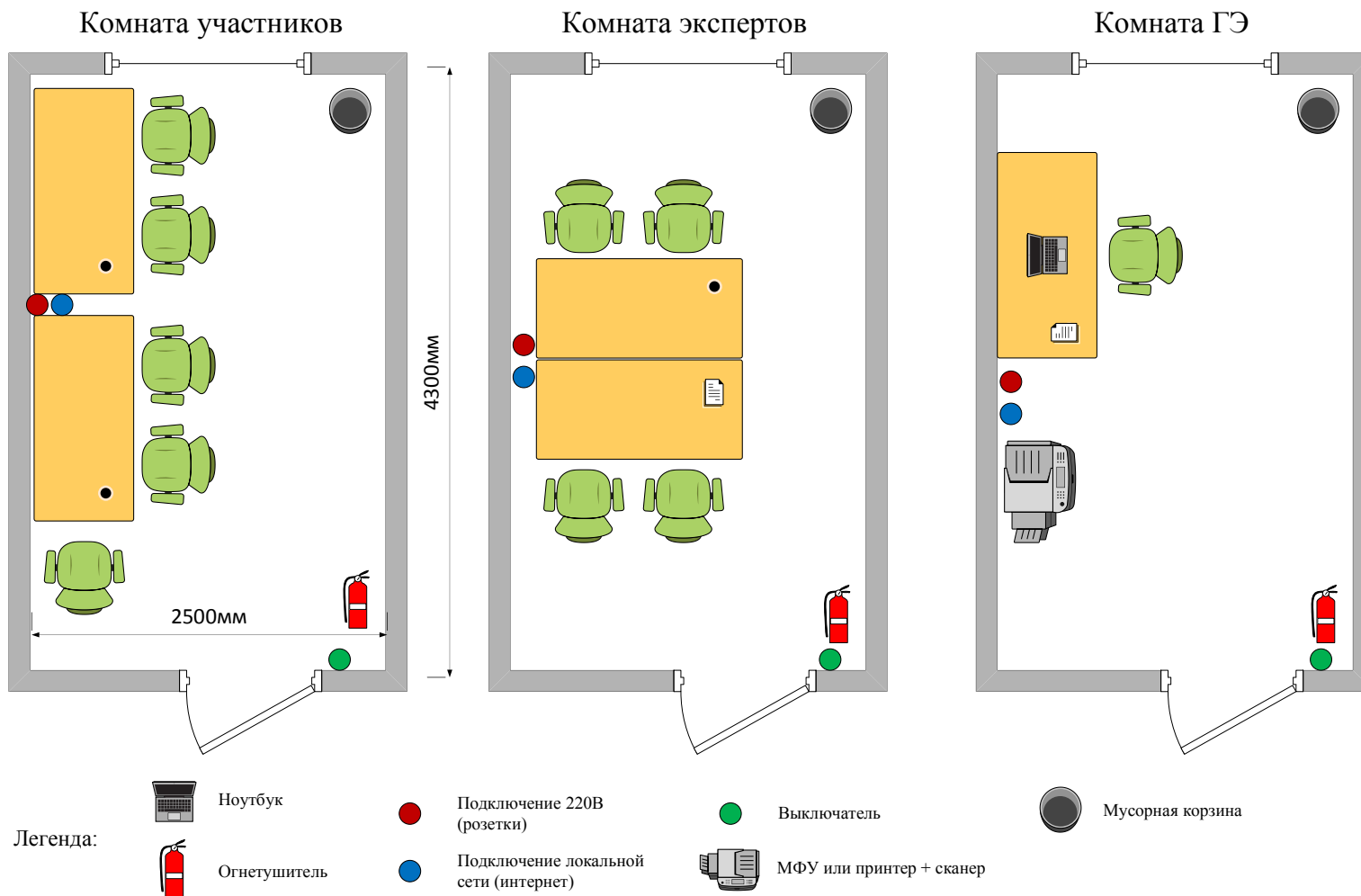
Приложение 5. План застройки площадки для проведения демонстрационного экзамена.

Приложение 6. Инфраструктурный(-ые) лист(-ы).

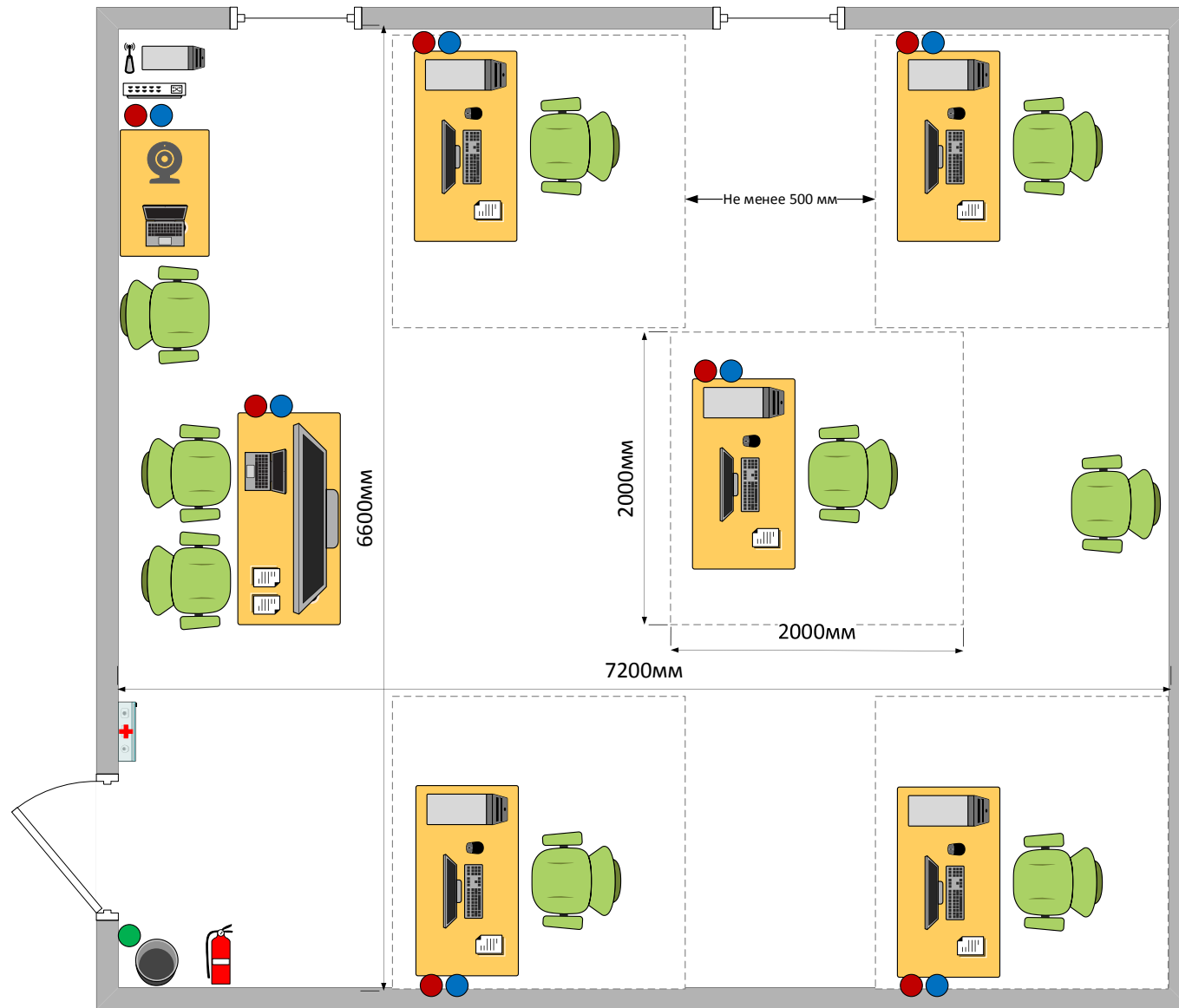
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный)

Формат проведения ДЭ: очный / распределенный

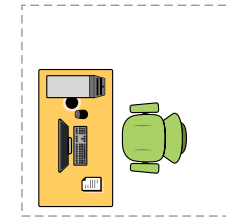
Общая площадь площадки: 80 м²



Площадка проведения экзамена



Легенда



Рабочее место (2×2 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, USB-накопитель, набор ПО



Ноутбук



Аптечка



Огнетушитель



ТВ/проектор
(таймер)



Камера (трансляция)



Сетевая инфраструктура
(сервер, коммутатор/
маршрутизатор, точка
доступа), может быть
в серверной



Подключение 220В
(розетки)



Подключение локальной
сети (интернет)



Выключатель



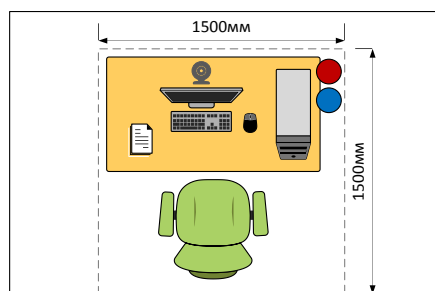
Мусорная корзина

План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (дистанционный)

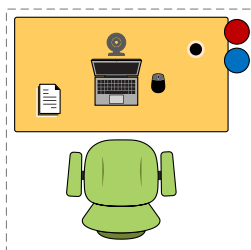
Формат проведения ДЭ: дистанционный

Общая площадь площадки: 2,25 м² (и более, на 1 участника/эксперта)

Рабочее место участника

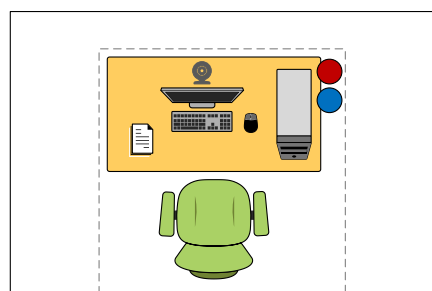


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

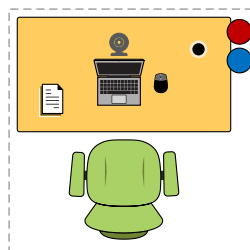


Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

Рабочее место эксперта

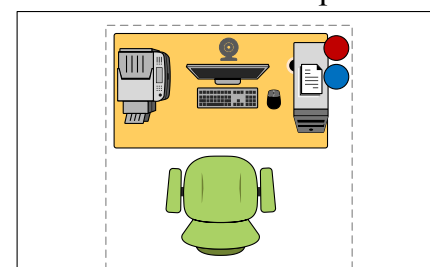


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

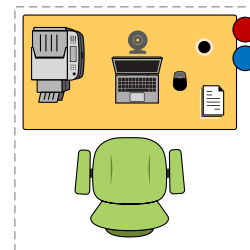


Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

Рабочее место главного эксперта

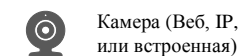


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, МФУ (принтер и сканер) или принтер + камера или смартфон (для «сканирования») набор ПО, доступ к Интернет (кабель или беспроводной)



Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, МФУ (принтер и сканер) или принтер + камера или смартфон (для «сканирования»), набор ПО, доступ к Интернет (кабель или беспроводной)

Легенда:



Камера (Веб, IP, или встроенная)



Подключение 220В (розетки)



Подключение локальной сети (интернет) или WiFi



МФУ или принтер + сканер, или принтер + камера/ смартфон/ планшет прочее с камерой

Образец задания

Образец задания для демонстрационного экзамена по комплексу оценочной документации.

Описание задания

Задание выполняется на подготовленных виртуальных машинах: контроллер домена с поднятым DNS и AD, серверная система в домене с установленным сервером агентского мониторинга, чистая клиентская система в домене (2 шт), предустановленный DLP-сервер (с установленной лицензией и LDAP-синхронизацией).

Перед экзаменом должны быть подготовлены следующие виртуальные машины для работы (рекомендуется сделать нулевой Snapshot для быстрой подготовки к другим потокам), сеть настроена в режиме NAT (сеть NAT) или Bridge с DHCP, с доступом в интернет, но без доступа к машинам других участников экзамена:

- AD и DNS сервер (контроллер домена), 1,5ГБ ОЗУ и выше, 2 ядра, статическая адресация с доступом в интернет,
- DLP сервер установлен (но не настроен), активирована лицензия, 6ГБ ОЗУ и выше, 2 ядра,
- Виртуальная машина с установленным сервером агентского мониторинга, 2ГБ ОЗУ и выше, 2 ядра,
- Виртуальные машины «нарушителей» (2 шт) введены в домен, 1,5ГБ ОЗУ и выше, 2 ядра.

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов (demo.lab, должен быть развернут из эталонного, получить эталон можно по запросу).

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными. При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и документацией на компьютерах.

Все дистрибутивы должны находиться в каталоге, указанном в карточке задания. Все логины, пароли, сетевые настройки и прочее, относящееся к инфраструктуре площадки, должно быть указано в карточке задания.

При создании снимков экрана необходимо делать либо полный снимок экрана, либо целого окна.

Описание модуля А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Задание 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “Test” в корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

Внутри созданного подразделения “Test” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: user1, пароль: ххХХ1234, права пользователя домена

Задание 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен и частично настроен.

Необходимо синхронизировать каталог LDAP.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» на рабочем столе компьютера.

Задание 3: Установка агента мониторинга на машине нарушителя

Установить агент мониторинга:

На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга.

Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания

Задание 4: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих некий термин, установить уровень угрозы для всех событий, добавить тег.

Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя 1 с установленным агентом.

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа, настроив конструктор выборки вручную.

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задание 5: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должны удовлетворять общепринятым на сегодня стандартам и требованиям, параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать:

1. корневой root-сертификат (ca)
2. серверный (server) сертификат
3. по желанию допускается использование пользовательского и промежуточного сертификата

Поля сертификата заполняются по вариантам заданий.

После генерации сертификатов необходимо установить корневой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети.

Итоговый результат должен включать:

Дерево из 2-3 сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе. Содержимое команд по генерации ключей и сертификатов в текстовом файле на рабочем столе с комментариями.

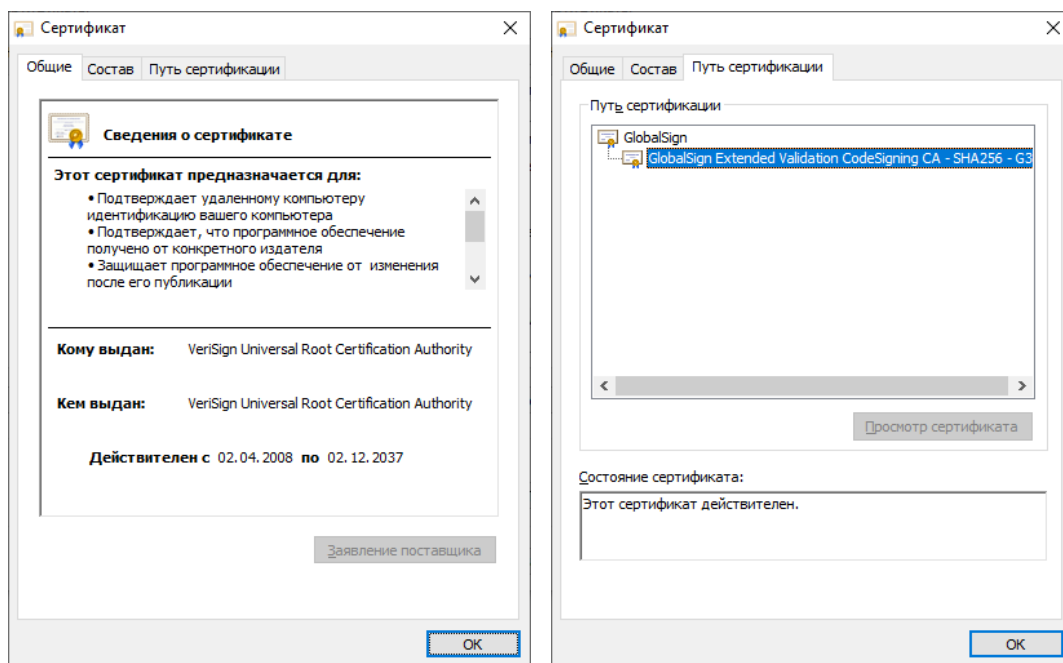


Рис1. Пример скриншотов задания

Описание модуля Е: Технологии защиты узла и агентский мониторинг

Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании). Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна. Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно).

Задание 1

Необходимо группу компьютеров: «Test1» и применить только на соответствующий компьютер.

Зафиксировать выполнение скриншотом.

Задание 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на другую машину для удаленного доступа к серверу агентского мониторинга.

Следующие правила создаются в политике «Test1».

Правило 1

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 3

Ограничить доступ к определенным облачным хранилищам (по вариантам).

Проверить работоспособность и зафиксировать выполнение

Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Правило 5

Необходимо запретить запись файлов на определенные носители информации, при этом оставить возможность считывания информации.

Проверить работоспособность и зафиксировать выполнение

Правило 6

С учетом ранее созданной блокировки необходимо разрешить использование доверенного носителя информации.

Проверить работоспособность и зафиксировать выполнение

Правило 7

Полностью запретить использование определенного устройства для пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 8

С учетом ранее выполненного запрета необходимо предоставить временный доступ для определенного устройства не определенное время для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Следующие правила создаются в политике «Test2».

Правило 9

Необходимо поставить на контроль буфер обмена в блокноте и notepad++. Проверить занесение нескольких событий в WEB-консоль.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 10

Запретить передачу файлов определенного типа на съемные носители информации или в сетевое расположение.

Проверить работоспособность и зафиксировать выполнение

Групповые политики домена

Групповые применяются только на компьютер 2, должны быть созданы в домене. Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например запрет запуска).

Групповая политика 1

Настроить политику паролей и блокировки: Максимальный срок действия пароля, Минимальная длина пароля, Сложность пароля, Блокировка учетной записи при неверном вводе пароля.

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Запретить запуск приложений по списку (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

Запретить использование элементов системы стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельно менять параметры системы (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Описание модуля С: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям. Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием. После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Для некоторых политик могут понадобиться дополнительные файлы, расположение которых можно узнать из карточки задания или у экспертов.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). Скриншоты необходимо сохранить в папке «Модуль 3».

Скриншоты необходимо называть в соответствии с номером задания и типом задания (Например Политика 2, Задание 1–1 и т. д.)

Задания на разработку политик можно выполнять в любом порядке.

Наиболее сложные политики находятся в конце.

При разработке политик стоит учитывать, что все политики трафика могут передаваться как через веб-сообщения, так и через почтовые сообщения. В случае, если данный пункт не соблюден, то проверка заданий может быть невозможной.

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации.

Список тегов для политик:

Политика 1, Политика 2, Политика 3, ...

Задание 1

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты.

Задание 2

Создайте локальную группу пользователей и добавьте в нее пользователей.

Задание 3

Создать список веб-ресурсов. Добавить в список следующие сайты: Site.ru, domain.com, ...

Задание 4

Для работы системы необходимо настроить периметр компании: Почтовый домен, Список веб ресурсов, Группа персон, Исключить из перехвата.

Политика 1

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела (по вариантам) отправлять документы, содержащие информацию о паспортных данных за пределы компании. Отдел (по вариантам) может отправлять файлы без ограничений.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 1

Политика 2

Для контроля за движением документов необходимо вести наблюдение за передачей шаблона документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах определенного уровня.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 2

Политика 3

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика.

Вердикт: заблокировать

Уровень нарушения: низкий

Тег: Политика 3

Политика 4

Необходимо отслеживать документы, содержащие печать компании всем сотрудникам, кроме отдела (по вариантам) и определенного сотрудника. Они могут обмениваться документами внутри и за пределами компании без контроля.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 4

Политика 5

Сотрудники заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из определенного отдела, для остальных контролировать не нужно.

Критичными данными в выгрузке являются определенные поля и в 1 документе присутствует более 1 строчки. Для настройки используйте файл примера.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 5

Политика 6

Некая компания попросила обеспечить защиту от утечки важных данных. Необходимо создать политику на контроль правила передачи содержащие слова «один», «два», «три» в 1 сообщении или документе одновременно. Если в

документе встречается только по 1 слову из перечисленных — политика срабатывать не должна.

Правило должно срабатывать на сообщения, которые отправляются за пределы компании всеми пользователями, кроме определенного отдела, который может отсылать информацию свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 6

Политика 7

Пользователи стали часто обмениваться ссылками и файлами, в связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов, например формата.mp4 и ссылок определенного формата (содержит уникальную последовательность, например urlname). Ложных срабатываний быть не должно.

Вердикт: Заблокировать

Уровень нарушения: средний

Тег: Политика 7

Политика 8

В связи с разгильдяйством сотрудников, передающих свои пароли коллегам с помощью почты и сообщений, необходимо предотвратить передачу любых стандартизированных паролей для информационной системы в открытом виде любыми отправителями и получателями как внутри, так и за пределы компании.

Стоит учесть, что пароли могут передаваться любым указанным способом: социальные сети и прочие ресурсы (в браузере), мессенджеры, почта, флешки. Необходимо также контролировать наличие паролей в сетевых каталогах.

Стоит учесть, что отдел так как генерацией паролей занимается отдел ИТ, то пользователи отдела могут рассылать пароли пользователям совершенно свободно, но только внутри компании.

Стандартизированные форматы паролей (кириллица):

6 букв – 1 знак !?#\$^/_& – 2-4 цифры – 4 буквы – 2-3 знака !?#\$^/_&
(например, ПаРоль#67pКнЕ!?)

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 8

Политика 9

Необходимо контролировать передачу определенных типов файлов только за пределы компании.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 9

Описание модуля F: Предотвращение инцидентов и управление событиями информационной безопасности

Задание 1: Контроль доступа

Необходимо создать пользователя DLP системы с определенными правами просмотра и редактирования.

Задание 2: Сводки

Создайте новые вкладки сводки в разделе «Сводка»

Задание 3: Виджеты

Создайте в сводке 4 виджета:

5. Выборка по событиям за период
6. Выборка по политикам с технологиями за период
7. Статистика за период
8. По нарушителям за период

Задание 4

Необходимо создать виджет отображающий события определенного типа (с определенного устройства и т. п.) за период.

Зафиксировать скриншотом конструктора выборки.

Задание 5

Необходимо создать виджет отображающий события определенного уровня (определенных политик и т. п.) за период.

Необходимые приложения

Приложение 1: Карточка настроек сети и оборудования (docx)

Приложение 2: Шаблоны документов для задания (zip)

5. Комплект оценочной документации паспорт КОД 1.4-2022

Паспорт комплекта оценочной документации

1. Описание

Комплект оценочной документации (КОД) разработан в целях организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия.

В данном разделе указаны основные характеристики КОД и должны использоваться при планировании, проведении и оценки результатов демонстрационного экзамена образовательными организациями, ЦПДЭ и Агентством.

Таблица 1. Паспорт комплекта оценочной документации (КОД)

№ п/п	Наименование	Информация о разработанном КОД
1	2	3
1	Номер компетенции	F7
2	Название компетенции	Корпоративная защита от внутренних угроз информационной безопасности
3	КОД является однодневным или двухдневным:	Однодневный
4	Номер КОД	КОД 1.4
4.1	Год(ы) действия КОД	2022 (1 год)
5	Уровень ДЭ	ФГОС СПО
6	Общее максимально возможное количество баллов задания по всем критериям оценки	27,00
7	Длительность выполнения экзаменационного задания данного КОД	4:30:00
8	КОД разработан на основе	ФНЧ Молодые профессионалы 2021
9	КОД подходит для проведения демонстрационного экзамена в качестве процедуры Независимой оценки квалификации (НОК)	НЕТ
10	Вид аттестации, для которой подходит данный КОД	Промежуточная
11	Формат проведения ДЭ	X
11.1	КОД разработан для проведения ДЭ в очном формате, (участники и эксперты находятся в ЦПДЭ)	Да
11.2	КОД разработан для проведения ДЭ в дистанционном формате, (участники и эксперты работают удаленно)	Не предусмотрено
11.3	КОД разработан для проведения ДЭ в распределенном формате, (детализация в п.11.3.1)	Не предусмотрено
11.3.1	Формат работы в распределенном формате	Не предусмотрено
12	Форма участия (индивидуальная, парная, групповая)	Индивидуальная

12.1	Количество человек в группе, (т.е. задание ДЭ выполняется индивидуально или в группе/ команде из нескольких экзаменуемых)	1,00
12.2	Организация работы при невозможности разбить экзаменуемых на указанное в п. 12.1 количество человек в группе	
13	Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3,00
16	Автоматизированная оценка результатов заданий	Автоматизация неприменима
16.1	Что автоматизировано: заполняется при выборе вариантов в п.16: возможна частичная или полная автоматизация	

2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта

Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта, (WorldSkills Standards Specification WSSS), проверяемый в рамках комплекта оценочной документации, (Таблица 2).

Таблица 2. WSSS

Номер раздела WSSS	Наименование раздела WSSS	Содержание раздела WSSS: Специалист должен знать	Важность раздела WSSS (%)
1	2	3	4
2	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	<p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> Сетевое окружение; Сетевые протоколы; Знать методы выявления и построения путей движения информации в организации; Подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия; Типы сетевых устройств; Разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз; Процесс выбора подходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем; Важность следования инструкциям и последствия, цену пренебрежения ими; Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы; Этапы установки системы корпоративной защиты от внутренних угроз; Знать отличия различных версий систем корпоративной защиты от внутренних угроз; Знать какие СУБД поддерживаются системой; Знать назначение различных компонент версий систем корпоративной защиты от внутренних угроз; Знать технологии программной и аппаратной виртуализации; Знать особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation; Цель документирования процессов обновления и установки. Важность спокойного и сфокусированного подхода к решению проблемы; 	14,00

		<p>Значимость систем ИТ-безопасности и зависимость пользователей и организаций от их доступности; Популярные аппаратные и программные ошибки; Знать разделы системы корпоративной безопасности, которые обычно использует системный администратор; Аналитический и диагностический подходы к решению проблем; Границы собственных знаний, навыков и полномочий; Ситуации, требующие вмешательства службы поддержки; Стандартное время решения наиболее популярных проблем. Специалист должен уметь: Интерпретировать пользовательские запросы и требования с точки зрения корпоративных требований; Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении; Настраивать сетевые устройства; Администрирование автоматизированных технические средства управления и контроля информации и информационных потоков; Навыки системного администрирования в операционных системах , Server, Linux (Red Hat Enterprise Linux, CentOS и др.); Навыки системного администрирования в защищенных операционных системах (AstraLinux и др.); Настройка в операционных системах прав доступа в соответствие с ролевой и/или мандатной моделью; Настройка средств виртуализации под операционными системам; Конфигурирование операционных систем для правильного и защищенного использования средств безопасности, в т.ч. системы корпоративной защиты от внутренних угроз.: Установка серверной части системы корпоративной защиты от внутренних угроз; Установка СУБД различного вида; Установка агентской части системы корпоративной защиты от внутренних угроз; Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом; Использовать дополнительные утилиты если это необходимо; Уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки; Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае</p>	
--	--	---	--

		<p>необходимости;</p> <p>Уметь сконфигурировать систему, чтобы она получала теневые копии;</p> <p>Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах;</p> <p>Демонстрировать уверенность и упорство в решении проблем;</p> <p>Быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы, точно описывать проблему и документировать её решение;</p> <p>Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей;</p> <p>Выбирать и принимать диагностирующее ПО и инструменты для поиска неисправностей;</p>	
6	Технологии защиты узла и агентского мониторинга	<p>Специалист должен знать и понимать:</p> <p>Функции агентского мониторинга;</p> <p>Общие настройки системы агентского мониторинга;</p> <p>Соединение с LDAP-сервером и синхронизация с Active Directory или функциональным аналогом;</p> <p>Политики агентского мониторинга, особенности их настройки;</p> <p>Особенности настроек событий агентского мониторинга;</p> <p>Механизмы диагностики агента, подходы к защите агента.</p> <p>Знать возможности и ограничения современных российских и зарубежных операционных систем в рамках решения задач защиты информации</p> <p>Знать архитектуру операционных систем</p> <p>Знать инструментарий по работа с современными операционными системами, команды, ПО, утилиты</p> <p>Специалист должен уметь:</p> <p>Установка и настройка агентского мониторинга;</p> <p>Создание политик защиты на агентах;</p> <p>Работа в консоли управления агентом;</p> <p>Фильтрация событий;</p> <p>Настройка совместных событий агентского и сетевого мониторинга;</p> <p>Работа с носителями и устройствами;</p> <p>Работа с файлами;</p> <p>Контроль приложений;</p> <p>Исключение из событий перехвата.</p> <p>Производить настройку сервисов и компонент операционной системы для достижения целей защиты</p> <p>Разделять компоненты операционной системы по уровням доверия, сокращая поверхность атаки для злоумышленника</p> <p>Применять механизмы ролевого и мандатного доступа и контроля целостности</p>	13,00

		Реализовывать ограниченную программную среду для пользователя Знать особенности безопасной работы и загрузки операционных систем на различных аппаратных платформах	
--	--	--	--

*Таблица соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами

доступна

в

Приложении

3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке

Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3
---	---

Соотношение количества экспертов в зависимости от количества экзаменуемых и количества рабочих мест.

Таблица 3. Расчет количества экспертов исходя из количества рабочих мест и участников.

Количество постов-рабочих мест на экзаменационной площадке	Количество участников <u>на одно пост-рабочее</u> место на одной экзаменационной площадке (по умолчанию 1 участник)	Максимальное количество участников в одной экзаменационной группе одной экзаменационной площадки	Количество экспертов на одну экзаменационную группу одной экзаменационной площадки
1	2	3	4
1	1	1	3
2	1	2	3
3	1	3	3
4	1	4	3
5	1	5	3
6	1	6	3
7	1	7	3
8	1	8	3
9	1	9	3
10	1	10	3
11	1	11	3
12	1	12	3
13	1	13	4
14	1	14	4
15	1	15	4
16	1	16	4
17	1	17	4
18	1	18	4
19	1	19	4
20	1	20	4
21	1	21	5
22	1	22	5
23	1	23	5
24	1	24	5
25	1	25	5

4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

По результатам выполнения заданий демонстрационного экзамена может быть применена схема перевода баллов из стобалльной шкалы в оценки по пятибалльной шкале.

Таблица 4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

Оценка	«2»	«3»	«4»	«5»
1	2	3	4	5
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00% - 19,99%	20,00% - 39,99%	40,00% - 69,99%	70,00% - 100,00%

5. Список оборудования и материалов, запрещенных на площадке (при наличии)

Таблица 5. Список оборудования и материалов, запрещенных на площадке, (при наличии)

№ п/п	Наименование запрещенного оборудования
1	2
1	Личный мобильный телефон (смартфон)
2	Наушники с передачей аудио (проводные, беспроводные)
3	Личный ноутбук
4	Личный планшет
5	Личная клавиатура
6	Личная компьютерная мышь

6. Детальная информация о распределении баллов и формате оценки.

Таблица 6. Обобщенная оценочная ведомость.

№ п/п	Модуль задания, где проверяется критерий	Критерий	Длительность модуля	Разделы WSSS	Судейские баллы	Объективные баллы	Общие баллы
1	2	3	4	5	6	7	8
1	А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	2:30:00	2	0,00	14,00	14,00
2	Е: Технологии защиты узла и агентского мониторинга	Технологии защиты узла и агентского мониторинга	2:00:00	6	0,00	13,00	13,00
Итого	-	-	4:30:00	-	0,00	27,00	27,00

7. Примерный план работы Центра проведения демонстрационного экзамена⁴.

Таблица 7. Примерный план работы Центра проведения демонстрационного экзамена.

День (выберете из выпадающего списка)	Начало мероприяти я (укажите в формате ЧЧ:ММ)	Окончание мероприяти я (укажите в формате ЧЧ:ММ)	Длительность мероприятия (расчет производится автоматически)	Мероприятие	Действия экспертной группы при распределенно м формате ДЭ (Заполняется при выборе распределенног о формата ДЭ)	Действия экзаменуемых при распределенном формате ДЭ (Заполняется при выборе распределенног о формата ДЭ)	Действия экспертной группы при дистанционном формате ДЭ (Заполняется при выборе дистанционног о формата ДЭ)	Действия экзаменуемых при дистанционном формате ДЭ (Заполняется при выборе дистанционног о формата ДЭ)
1	2	3	4	5	6	7	8	9
Подготовительны й день (С-1)	09:00:00	09:15	0:15:00	Получение главным экспертом задания демонстрационног о экзамена				
Подготовительны й день (С-1)	09:15:00	10:00:00	0:45:00	Проверка готовности проведения демонстрационног о экзамена, заполнение Акта о готовности площадки				
Подготовительны й день (С-1)	10:00:00	10:15:00	0:15:00	Распределение обязанностей по				

⁴ Если планируется проведение демонстрационного экзамена для двух и более экзаменационных групп (ЭГ) из одной учебной группы одновременно на одной площадке, то это также должно быть отражено в плане. Примерный план рекомендуется составить таким образом, чтобы продолжительность работы экспертов на площадке не превышала нормы, установленные действующим законодательством. В случае необходимости превышения установленной продолжительности по объективным причинам, требуется согласование с экспертами, задействованными для работы на соответствующей площадке.

				проведению экзамена между членами Экспертной группы, заполнение протоколов				
Подготовительный день (С-1)	10:15:00	10:30:00	0:15:00	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах				
Подготовительный день (С-1)	10:30:00	10:45:00	0:15:00	Регистрация участников демонстрационного экзамена				
Подготовительный день (С-1)	10:45:00	11:15:00	0:30:00	Инструктаж участников по охране труда и технике безопасности, сбор подписей в протоколах				
Подготовительный день (С-1)	11:15:00	13:00:00	1:45:00	Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и				

				заполнение протоколов				
Подготовительный день (С-1)	13:00:00	16:00:00	3:00:00	Подготовка и/или проверка работоспособности площадки в соответствии с заданием				
День 1	08:45:00	09:00:00	0:15:00	Ознакомление с заданием и правилами				
День 1	09:00:00	09:15:00	0:15:00	Брифинг				
День 1	09:15:00	10:45:00	1:30:00	Выполнение модуля А				
День 1	10:45:00	11:00:00	0:15:00	Перерыв, обработка помещения, проветривание				
День 1	11:00:00	12:00:00	1:00:00	Выполнение модуля А				
День 1	12:00:00	12:45:00	0:45:00	Обед, обработка помещения, проветривание				
День 1	12:45:00	14:45:00	2:00:00	Выполнение модуля Е				
День 1	14:45:00	17:15:00	2:30:00	Работа экспертов, заполнение форм и оценочных ведомостей				
День 1	17:15:00	18:15:00	1:00:00	Подведение итогов, внесение главным экспертом баллов				

				в CIS, сверка баллов				
--	--	--	--	-------------------------	--	--	--	--

8. Необходимые приложения

Приложение 2. Соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами.

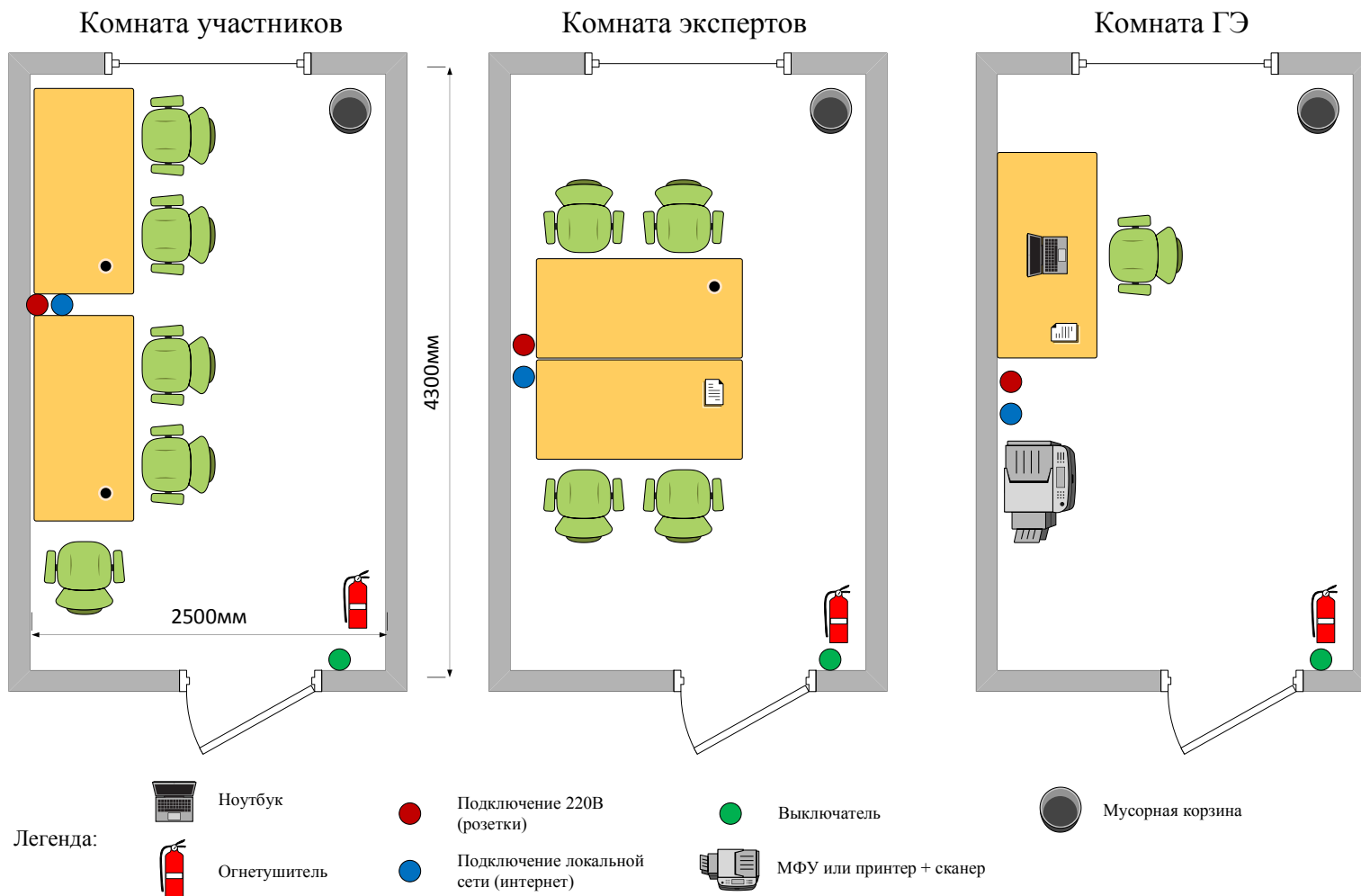
Приложение 5. План застройки площадки для проведения демонстрационного экзамена.

Приложение 6. Инфраструктурный(-ые) лист(-ы).

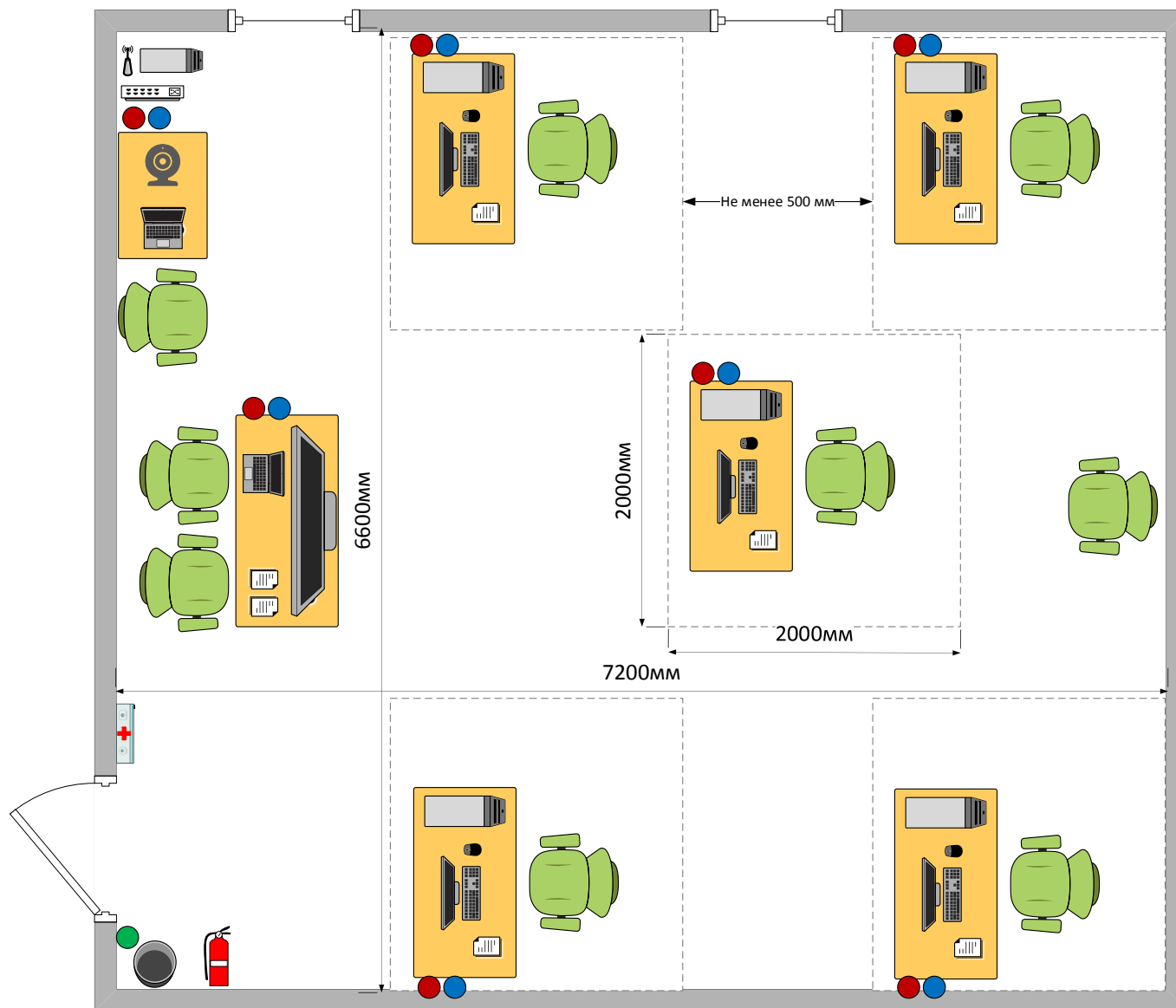
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный)

Формат проведения ДЭ: очный / распределенный

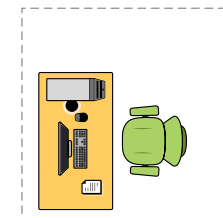
Общая площадь площадки: 80 м²



Площадка проведения экзамена



Легенда



Рабочее место (2×2 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, USB-накопитель, набор ПО



Ноутбук



Аптечка



Огнетушитель



ТВ/проектор (таймер)



Камера (трансляция)



Сетевая инфраструктура (сервер, коммутатор/маршрутизатор, точка доступа), может быть в серверной



Подключение 220В (розетки)



Подключение локальной сети (интернет)



Выключатель



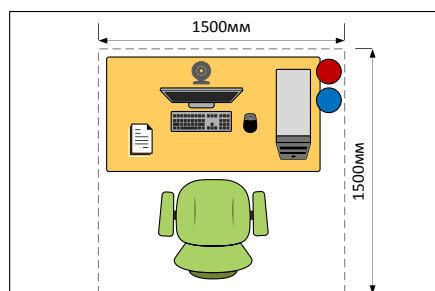
Мусорная корзина

План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (дистанционный)

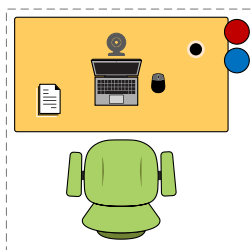
Формат проведения ДЭ: дистанционный

Общая площадь площадки: 2,25 м² (и более, на 1 участника/эксперта)

Рабочее место участника

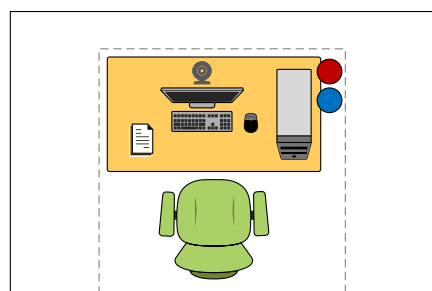


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

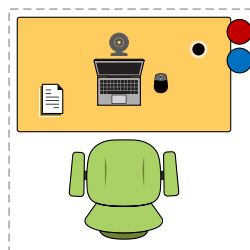


Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

Рабочее место эксперта

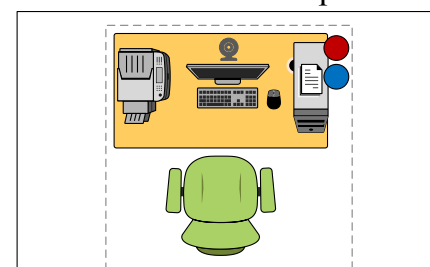


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

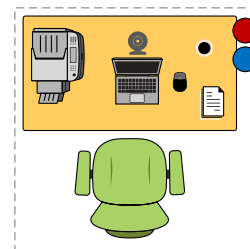


Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

Рабочее место главного эксперта

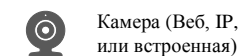


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, МФУ (принтер и сканер) или принтер + камера или смартфон (для «сканирования») набор ПО, доступ к Интернет (кабель или беспроводной)



Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, МФУ (принтер и сканер) или принтер + камера или смартфон (для «сканирования»), набор ПО, доступ к Интернет (кабель или беспроводной)

Легенда:



Камера (Веб, IP, или встроенная)



Подключение 220В (розетки)



Подключение локальной сети (интернет) или WiFi



МФУ или принтер + сканер, или принтер + камера/ смартфон/ планшет прочее с камерой

Образец задания

Образец задания для демонстрационного экзамена по комплекту оценочной документации.

Описание задания

На площадке должна быть развернута сеть с доступом в Интернет.

Необходимо предоставить дистрибутивы Astra Linux SE 1.6 или функциональный аналог и выше, дистрибутивы DLP системы под данную версию, образ обновления безопасности ОС, образ средств разработчика и образ обновления средств разработчика. Все дистрибутивы и обновления должны быть совместимы.

Компания «Демо Лаб» запланировала переход на отечественное программное обеспечение. Для перехода был выбран на первом этапе один офис в качестве тестирования.

В качестве домена принято решение установить и настроить ALD домен, поднятый на Linux.

Вам необходимо настроить сеть на предполагаемом ALD домене и рабочих станциях под управлением операционной системы Linux в соответствии с выданным заданием, настроить различные политики и установить DLP систему на Linux.

Для большей сетевой безопасности в компании все устройства должны иметь статический IP-адрес. Сетевые настройки указаны в дополнительных сведениях к заданию.

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными в соответствии с рабочим местом (например, server8).

Перед установкой систем стоит убедиться в правильности настройки сети на гипервизорах.

При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и документацией на компьютерах.

Все дистрибутивы находятся в каталоге, указанном в дополнительной карточке задания. Все логины, пароли, сетевые настройки и прочее указаны в дополнительной карточке задания

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например: Задание_5.jpg, все скриншоты и отчеты сохраняются на рабочий стол физического компьютера в папки по названию модулей (например Модуль 1) или передаются экспертам иным способом по запросу.

Описание модуля А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Задание 1, установка

Необходимо установить 3 (три) виртуальные машины с Linux.

При установке каждой машины необходимо создать стандартного пользователя с паролем

Рекомендуется устанавливать машины с графическим интерфейсом, т. к. на контроллере домена необходим будет браузер.

Машина 1, роль ALD-сервера, машина 2, роль ALD клиента (для работы в домене)

Машина 3, роль ALD клиента (для работы в домене и установки DLP системы)

Для данной машины (dlp) необходимо иметь 4 образа: установочный для системы, обновление системы, образ разработчика и образ обновлений разработчика той же версии, что и образ обновлений системы. Версии выбираются в соответствии с документацией на версию DLP системы.

Установку необходимо произвести со стандартными настройками, не включать дополнительные режимы безопасности.

Установка некоторых машин может быть произведена клонированием существующих.

Адреса систем выбираются самостоятельно в соответствии с карточкой задания.

Все адреса, имена и логины-пароли систем должны быть внесены в файл «отчет.txt» на рабочем столе компьютера!

Задание 2, развертывание домена

На ALD сервере необходимо развернуть ALD-домен

В домене необходимо создать пользователей:

Основной администратор домена

Логин: user1, установить МРД уровня целостности, доступ на компьютер

Логин: user2, права пользователя домена, разрешить доступ на компьютер

Логин: user3, установить МРД категорию 0 и 1, дать пользователю привилегию менять мандатные метки файлов.

Ввести машины в домен, продолжить работу под соответствующими пользователями.

Выполнение задания зафиксировать скриншотами.

Задание 3, настройка сети и удаленного доступа

Включить возможность SSH соединения на всех машинах.

Так как стандартный порт SSH-соединения подвержен атакам необходимо изменить стандартный порт на порт и проверить его работоспособность. Сохранить скриншот об удачном SSH-соединении по порту.

Ограничьте доступ по SSH-соединению отовсюду кроме доверенных IP-адресов (адресного пространства всех виртуальных машин).

Проверьте выполнение и зафиксируйте скриншотом.

Поставьте ограничения на подключение к SSH-соединению для усложнения подбора пароля. Зафиксируйте выполнение скриншотом.

Откройте порт для доверенных IP-адресов (домена) на машине.

Зафиксируйте выполнение скриншотами.

Задание 4, NTP

Необходимо поднять сервер времени для работоспособности DLP системы.

Сервер времени должен сообщать точное время машинам в сети (открыть доступ если требуется. Синхронизировать сам NTP сервер можно либо с гипервизором, либо с сервером точного времени в сети Интернет (локальной сети, если имеется).

Зафиксируйте выполнение скриншотом.

Задание 5, установка DLP сервера

Необходимо установить DLP сервер DLP-системы уровня сети.

Перед установкой необходимо настроить репозитории в соответствии с документацией на DLP-систему.

Скопировать файлы установки системы можно любым способом.

Установку необходимо произвести со следующими параметрами:

- Все в одном
- Параметры интерфейса и БД (PostgreSQL или функциональный аналог)

После установки системы необходимо перейти в Веб-консоль и убедиться в ее работоспособности.

Задание 6, настройка DLP сервера

Необходимо настроить LDAP синхронизацию с доменом. Для подключения использовать ранее созданного пользователя.

Зафиксировать настройки и результат скриншотом.

Настроить управление веб-консолью от пользователя. Установить полные права, все области видимости.

Зафиксировать настройки и результат скриншотом.

Задание 7, защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должны удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности не более 1 года, длине ключа не менее 2048 бит и т. п.), параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать:

- корневой root-сертификат (ca)
- серверный (server) сертификат
- по желанию допускается использование пользовательского и промежуточного сертификата

Дополнительная информация сертификатов должна включать в себя:

- Страна:
- Город
- Компания (и иные дополнительные поля)
- Отдел
- Почтовый адрес
- Пароли ключей

Остальные поля заполняются самостоятельно.

После генерации сертификатов необходимо установить серверный сертификат на веб-сервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена (и/или в браузер) для доверенного подключения к веб-консоли DLP-системы уровня сети.

Итоговый результат должен включать:

Дерево из 2-3 сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе в каталоге «Сертификаты»

Содержимое команд по генерации ключей и сертификатов в текстовом файле «сертификаты.txt» на рабочем столе с комментариями.

Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).

Сертификаты не должны содержать ошибок, предупреждений (warnings), неверной информации о компании и т. п.

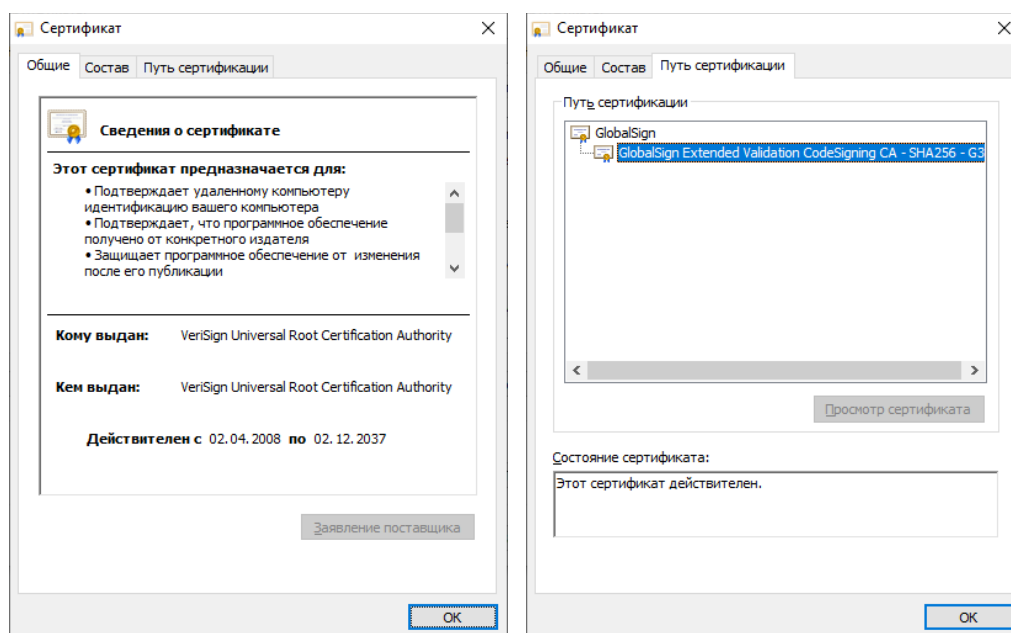


Рисунок 1. Пример скриншотов задания

Описание модуля Е: Технологии защиты узла и агентский мониторинг

В домене необходимо настроить следующие политики:

Политика 1

Для пользователей домена поставить количество неуспешных попыток входа, период блокировки учётной записи.

Выполнение зафиксировать скриншотом.

Политика 2

Определить локальную политику паролей.

Выполнение зафиксировать скриншотом.

Политика 3

Запретить использование компонентов доменным пользователям.

Выполнение зафиксировать скриншотом.

Политика 4

Разрешить производить некоторые действия только администратору.

Выполнение зафиксировать скриншотом.

Политика 5

Создать следующие уровни конфиденциальности:

- 0
- 1
- 2

Применить к пользователю уровень конфиденциальности.

Выполнение зафиксировать скриншотом.

Задание 6

На домене создать новый диск на, разметить его в режиме LVM и создать зашифрованный раздел с точкой монтирования (в любом каталоге).

Раздел должен автоматически загружаться и монтироваться при загрузке системы.

Выполнение заданий и результаты подтвердить скриншотом.

Задание 7

На домене на зашифрованном разделе создать сетевой ресурс (NFS, Samba), положить внутрь файл.

Для файла применить мандатную метку.

Создать цифровую подпись и подписать созданный ранее договор цифровой подписью. Установить пароль для цифровой подписи.

Выполнение задания подтвердить скриншотами: наличие ключа; информация о подписании договора и верной цифровой подписи

Проверить видимость сетевого ресурса на компьютере. Выполнение заданий и результаты подтвердить скриншотом.

Задание 8

Установить сервер агентского мониторинга на развернутый сервер.

Подключить сервер агентского мониторинга к ранее развернутому DLP-серверу.

Произвести синхронизацию с LDAP (пользователи).

Выполнение заданий и результаты подтвердить скриншотом.

Задание 9

Установить агент мониторинга на машину.

Убедиться, что клиент появился в консоли сервера агентского мониторинга.

Для проверки работоспособности создать любую политику, проверить ее, зафиксировать выполнение скриншотами.

Задание 10

Необходимо создать скрипт, который автоматически выводит в первую текстовую консоль пользователя (tty) информацию.

Формат выбора выбрать самостоятельно. Скрипт должен работать даже после перезагрузки системы.

Выполнение заданий и результаты подтвердить скриншотом.

Необходимые приложения

Приложение 1: Карточка настроек сети и оборудования (docx)

6. Комплект оценочной документации паспорт КОД 1.5– 2022

Паспорт комплекта оценочной документации

1. Описание

Комплект оценочной документации (КОД) разработан в целях организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия.

В данном разделе указаны основные характеристики КОД и должны использоваться при планировании, проведении и оценки результатов демонстрационного экзамена образовательными организациями, ЦПДЭ и Агентством.

Таблица 1. Паспорт комплекта оценочной документации (КОД)

№ п/п	Наименование	Информация о разработанном КОД
1	2	3
1	Номер компетенции	F7
2	Название компетенции	Корпоративная защита от внутренних угроз информационной безопасности
3	КОД является однодневным или двухдневным:	Однодневный
4	Номер КОД	КОД 1.5
4.1	Год(ы) действия КОД	2022 (1 год)
5	Уровень ДЭ	ФГОС СПО
6	Общее максимально возможное количество баллов задания по всем критериям оценки	27,00
7	Длительность выполнения экзаменационного задания данного КОД	5:30:00
8	КОД разработан на основе	ФНЧ Молодые профессионалы 2021
9	КОД подходит для проведения демонстрационного экзамена в качестве процедуры Независимой оценки квалификации (НОК)	НЕТ
10	Вид аттестации, для которой подходит данный КОД	Промежуточная
11	Формат проведения ДЭ	X
11.1	КОД разработан для проведения ДЭ в очном формате, (участники и эксперты находятся в ЦПДЭ)	Да
11.2	КОД разработан для проведения ДЭ в дистанционном формате, (участники и эксперты работают удаленно)	Не предусмотрено
11.3	КОД разработан для проведения ДЭ в распределенном формате, (детализация в п.11.3.1)	Не предусмотрено
11.3.1	Формат работы в распределенном формате	Участники находятся в ЦПДЭ, эксперты работают удаленно
12	Форма участия (индивидуальная, парная, групповая)	Индивидуальная

12.1	Количество человек в группе, (т.е. задание ДЭ выполняется индивидуально или в группе/ команде из нескольких экзаменуемых)	1,00
12.2	Организация работы при невозможности разбить экзаменуемых на указанное в п. 12.1 количество человек в группе	
13	Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3,00
16	Автоматизированная оценка результатов заданий	Автоматизация неприменима
16.1	Что автоматизировано: заполняется при выборе вариантов в п.16: возможна частичная или полная автоматизация	

2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта

Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта, (WorldSkills Standards Specification WSSS), проверяемый в рамках комплекта оценочной документации, (Таблица 2).

Таблица 2. WSSS

Номер раздела WSSS	Наименование раздела WSSS	Содержание раздела WSSS: Специалист должен знать	Важность раздела WSSS (%)
1	2	3	4
2	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	Специалист должен знать и понимать:Сетевое окружение; Сетевые протоколы; Знать методы выявления и построения путей движения информации в организации;Подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия; Типы сетевых устройств;Разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз; Процесс выбора подходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем; Важность следования инструкциям и последствия, цену пренебрежения ими; Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы; Этапы установки системы корпоративной защиты от внутренних угроз;Знать отличия различных версий систем корпоративной защиты от внутренних угроз;Знать какие СУБД поддерживаются системой;Знать назначение различных компонент версий систем корпоративной защиты от внутренних угроз;Знать технологии программной и аппаратной виртуализации;Знать особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation;Цель документирования процессов обновления и установки.Важность спокойного и сфокусированного подхода к решению проблемы; Значимость систем ИТ-безопасности и зависимость пользователей и организаций от их доступности; Популярные аппаратные и программные ошибки; Знать разделы системы корпоративной безопасности, которые обычно использует системный администратор;Аналитический и диагностический подходы к решению проблем; Границы собственных знаний, навыков и полномочий; Ситуации, требующие вмешательства службы поддержки; Стандартное время решения наиболее популярных проблем.Специалист должен уметь:Интерпретировать пользовательские запросы и требования с точки зрения корпоративных	8,00

		<p>требований; Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении; Настраивать сетевые устройства; Администрирование автоматизированных технических средства управления и контроля информации и информационных потоков; Навыки системного администрирования в операционных системах Windows, Windows Server, Linux (Red Hat Enterprise Linux, CentOS и др.); Навыки системного администрирования в защищенных операционных системах (AstraLinux и др.); Настройка в операционных системах прав доступа в соответствие с ролевой и/или мандатной моделью; Настройка средств виртуализации под операционными системам; Конфигурирование операционных систем для правильного и защищенного использования средств безопасности, в т.ч. системы корпоративной защиты от внутренних угроз.; Установка серверной части системы корпоративной защиты от внутренних угроз; Установка СУБД различного вида; Установка агентской части системы корпоративной защиты от внутренних угроз; Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом; Использовать дополнительные утилиты если это необходимо; Уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки; Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае необходимости; Уметь сконфигурировать систему, чтобы она получала теневые копии; Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах; Демонстрировать уверенность и упорство в решении проблем; Быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы, точно описывать проблему и документировать её решение; Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей; Выбирать и принимать диагностирующее ПО и инструменты для поиска неисправностей;</p>	
6	Технологии защиты узла и агентского мониторинга	<p>Специалист должен знать и понимать: Функции агентского мониторинга; Общие настройки системы агентского мониторинга; Соединение с LDAP-сервером и синхронизация с Active Directory; Политики агентского мониторинга, особенности их настройки; Особенности настроек событий агентского мониторинга; Механизмы диагностики агента, подходы к защите агента. Знать возможности и ограничения современных российских и зарубежных операционных систем в рамках решения задач защиты информации. Знать архитектуру операционных систем. Знать инструментарий по работе с современными операционными системами, команды, ПО, утилиты. Специалист</p>	4,00

		должен уметь: Установка и настройка агентского мониторинга; Создание политик защиты на агентах; Работа в консоли управления агентом; Фильтрация событий; Настройка совместных событий агентского и сетевого мониторинга; Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата. Производить настройку сервисов и компонент операционной системы для достижения целей защиты; Разделять компоненты операционной системы по уровням доверия, сокращая поверхность атаки для злоумышленника; Применять механизмы ролевого и мандатного доступа и контроля целостности; Реализовывать ограниченную программную среду для пользователя; Знать особенности безопасной работы и загрузки операционных систем на различных аппаратных платформах	
7	Предотвращение инцидентов и управление событиями информационной безопасности	Специалист должен знать и понимать: Назначение, роль, возможности систем IDS/IPS для задачи защиты организации от угроз информационной безопасности; Назначение, роль, возможности систем SIEM для задачи защиты организации от угроз информационной безопасности; Назначение, роль, возможности систем Threat Intelligence для задачи защиты организации от угроз информационной безопасности. Специалист должен уметь: Устанавливать, настраивать системы IDS/IPS; Устанавливать, настраивать системы SIEM; Устанавливать, настраивать системы Threat Intelligence, генерации трафика и проверки защищенности; Применять на практике системы IDS/IPS для выявления инцидентов информационной безопасности. Применять на практике системы Threat Intelligence. Применять на практике системы Threat Intelligence и Attack Simulation (Breach and Attack Simulation) для проверки/оценки устойчивости систем и сетей к компьютерным атакам. Проводить анализ выявленных инцидентов, использовать встроенные и внешние системы подготовки отчетности	15,00

*Таблица соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами

доступна

в

Приложении

3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке

Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3
---	---

Соотношение количества экспертов в зависимости от количества экзаменуемых и количества рабочих мест.

Таблица 3. Расчет количества экспертов исходя из количества рабочих мест и участников.

Количество постов-рабочих мест на экзаменационной площадке	Количество участников <u>на одно пост-рабочее</u> место на одной экзаменационной площадке (по умолчанию 1 участник)	Максимальное количество участников в одной экзаменационной группе одной экзаменационной площадки	Количество экспертов на одну экзаменационную группу одной экзаменационной площадки
1	2	3	4
1	1	1	3
2	1	2	3
3	1	3	3
4	1	4	3
5	1	5	3
6	1	6	3
7	1	7	3
8	1	8	3
9	1	9	3
10	1	10	3
11	1	11	3
12	1	12	3
13	1	13	4
14	1	14	4
15	1	15	4
16	1	16	4
17	1	17	4
18	1	18	4
19	1	19	4
20	1	20	4
21	1	21	5
22	1	22	5
23	1	23	5
24	1	24	5
25	1	25	5

4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

По результатам выполнения заданий демонстрационного экзамена может быть применена схема перевода баллов из стобалльной шкалы в оценки по пятибалльной шкале.

Таблица 4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

Оценка	«2»	«3»	«4»	«5»
1	2	3	4	5
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00% - 19,99%	20,00% - 39,99%	40,00% - 69,99%	70,00% - 100,00%

5. Список оборудования и материалов, запрещенных на площадке (при наличии)

Таблица 5. Список оборудования и материалов, запрещенных на площадке, (при наличии)

№ п/п	Наименование запрещенного оборудования
1	2
1	Личный мобильный телефон (смартфон)
2	Наушники с передачей аудио (проводные, беспроводные)
3	Личный ноутбук
4	Личный планшет
5	Личная клавиатура
6	Личная компьютерная мышь

6. Детальная информация о распределении баллов и формате оценки.

Таблица 6. Обобщенная оценочная ведомость.

№ п/п	Модуль задания, где проверяется критерий	Критерий	Длительность модуля	Разделы WSSS	Судейские баллы	Объективные баллы	Общие баллы
1	2	3	4	5	6	7	8
1	А: Установка, конфигурирование и устранение неисправностей в системе предотвращения вторжений	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	1:30:00	2	0,00	8,00	8,00
2	Ф: Предотвращение инцидентов и управление событиями информационной безопасности	Предотвращение инцидентов и управление событиями информационной безопасности	3:30:00	7	0,00	15,00	15,00
3	Е: Технологии защиты узла и агентского мониторинга	Технологии защиты узла и агентского мониторинга	0:30:00	6	0,00	4,00	4,00
Итого	-	-	5:30:00	-	0,00	27,00	27,00

7. Примерный план работы Центра проведения демонстрационного экзамена⁵.

Таблица 7. Примерный план работы Центра проведения демонстрационного экзамена.

День (выберете из выпадающего списка)	Начало мероприяти я (укажите в формате ЧЧ:ММ)	Окончание мероприяти я (укажите в формате ЧЧ:ММ)	Длительность мероприятия (расчет производится автоматически)	Мероприятие	Действия экспертной группы при распределенном формате ДЭ (Заполняется при выборе распределенног о формата ДЭ)	Действия экзаменуемых при распределенном формате ДЭ (Заполняется при выборе распределенног о формата ДЭ)	Действия экспертной группы при дистанционном формате ДЭ (Заполняется при выборе дистанционног о формата ДЭ)	Действия экзаменуемых при дистанционном формате ДЭ (Заполняется при выборе дистанционног о формата ДЭ)
1	2	3	4	5	6	7	8	9
Подготовительны й день (С-1)	09:00:00	09:15	0:15:00	Получение главным экспертом задания демонстрационн о экзамена				
Подготовительны й день (С-1)	09:15:00	10:00:00	0:45:00	Проверка готовности проведения демонстрационн о экзамена, заполнение Акта о готовности площадки				
Подготовительны й день (С-1)	10:00:00	10:15:00	0:15:00	Распределение обязанностей по				

⁵ Если планируется проведение демонстрационного экзамена для двух и более экзаменационных групп (ЭГ) из одной учебной группы одновременно на одной площадке, то это также должно быть отражено в плане. Примерный план рекомендуется составить таким образом, чтобы продолжительность работы экспертов на площадке не превышала нормы, установленные действующим законодательством. В случае необходимости превышения установленной продолжительности по объективным причинам, требуется согласование с экспертами, задействованными для работы на соответствующей площадке.

				проведению экзамена между членами Экспертной группы, заполнение протоколов				
Подготовительный день (С-1)	10:15:00	10:30:00	0:15:00	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах				
Подготовительный день (С-1)	10:30:00	10:45:00	0:15:00	Регистрация участников демонстрационного экзамена				
Подготовительный день (С-1)	10:45:00	11:15:00	0:30:00	Инструктаж участников по охране труда и технике безопасности, сбор подписей в протоколах				
Подготовительный день (С-1)	11:15:00	13:00:00	1:45:00	Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и				

				заполнение протоколов				
Подготовительный день (С-1)	13:00:00	16:00:00	3:00:00	Подготовка и/или проверка работоспособности площадки в соответствии с заданием				
День 1	08:45:00	09:00:00	0:15:00	Ознакомление с заданием и правилами				
День 1	09:00:00	09:15:00	0:15:00	Брифинг				
День 1	09:15:00	10:45:00	1:30:00	Выполнение модуля А				
День 1	10:45:00	11:00:00	0:15:00	Перерыв, обработка помещения, проветривание				
День 1	11:00:00	13:00:00	2:00:00	Выполнение модуля F				
День 1	13:00:00	13:45:00	0:45:00	Обед, обработка помещения, проветривание				
День 1	13:45:00	15:15:00	1:30:00	Выполнение модуля F				
День 1	15:15:00	15:30:00	0:15:00	Перерыв, обработка помещения, проветривание				
День 1	15:30:00	16:00:00	0:30:00	Выполнение модуля Е				
День 1	16:00:00	18:30:00	2:30:00	Работа экспертов, заполнение форм и				

				оценочных ведомостей				
День 1	18:30:00	19:30:00	1:00:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение протоколов				

8. Необходимые приложения

Приложение 2. Соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами.

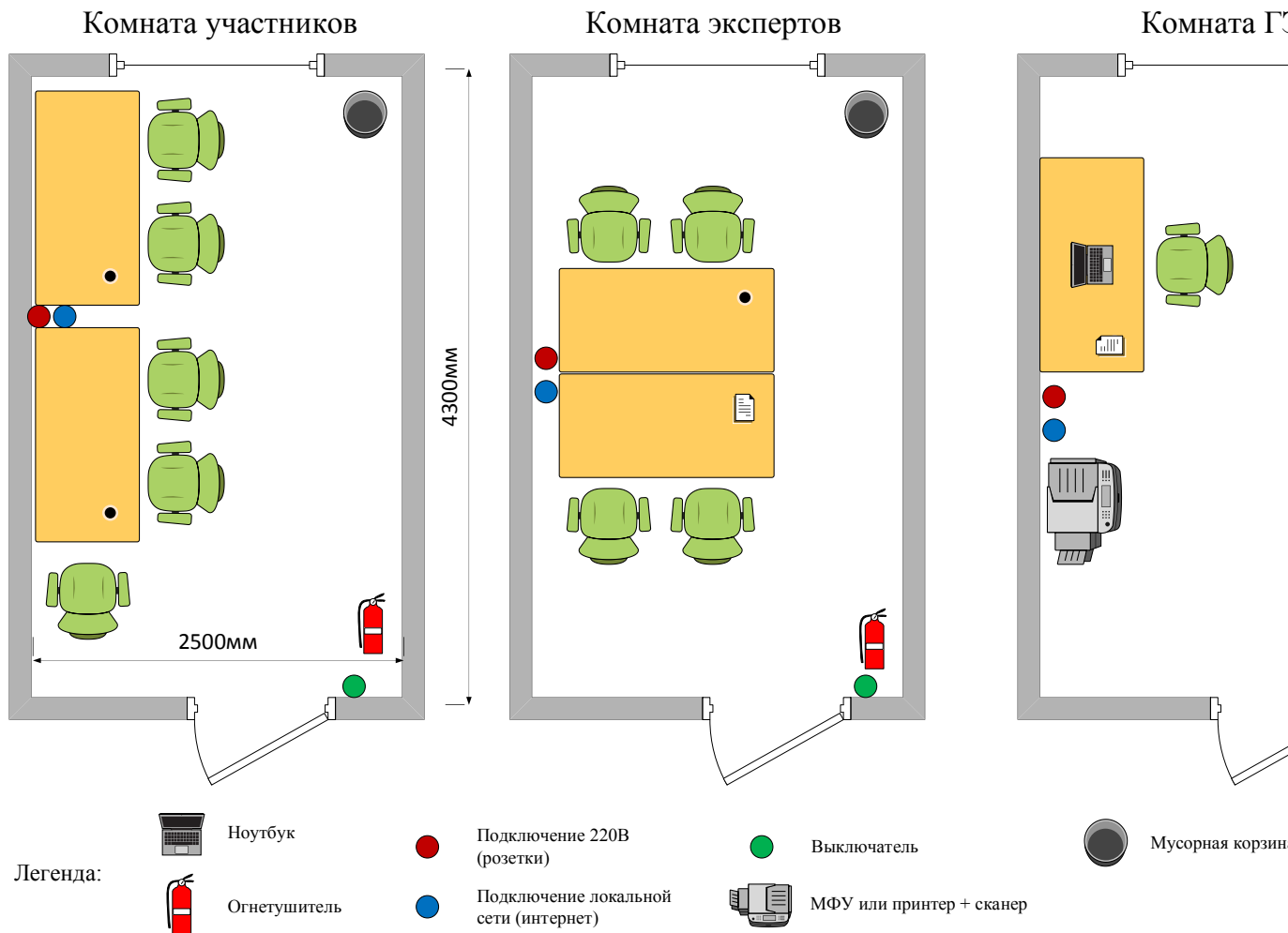
Приложение 5. План застройки площадки для проведения демонстрационного экзамена.

Приложение 6. Инфраструктурный(-ые) лист(-ы).

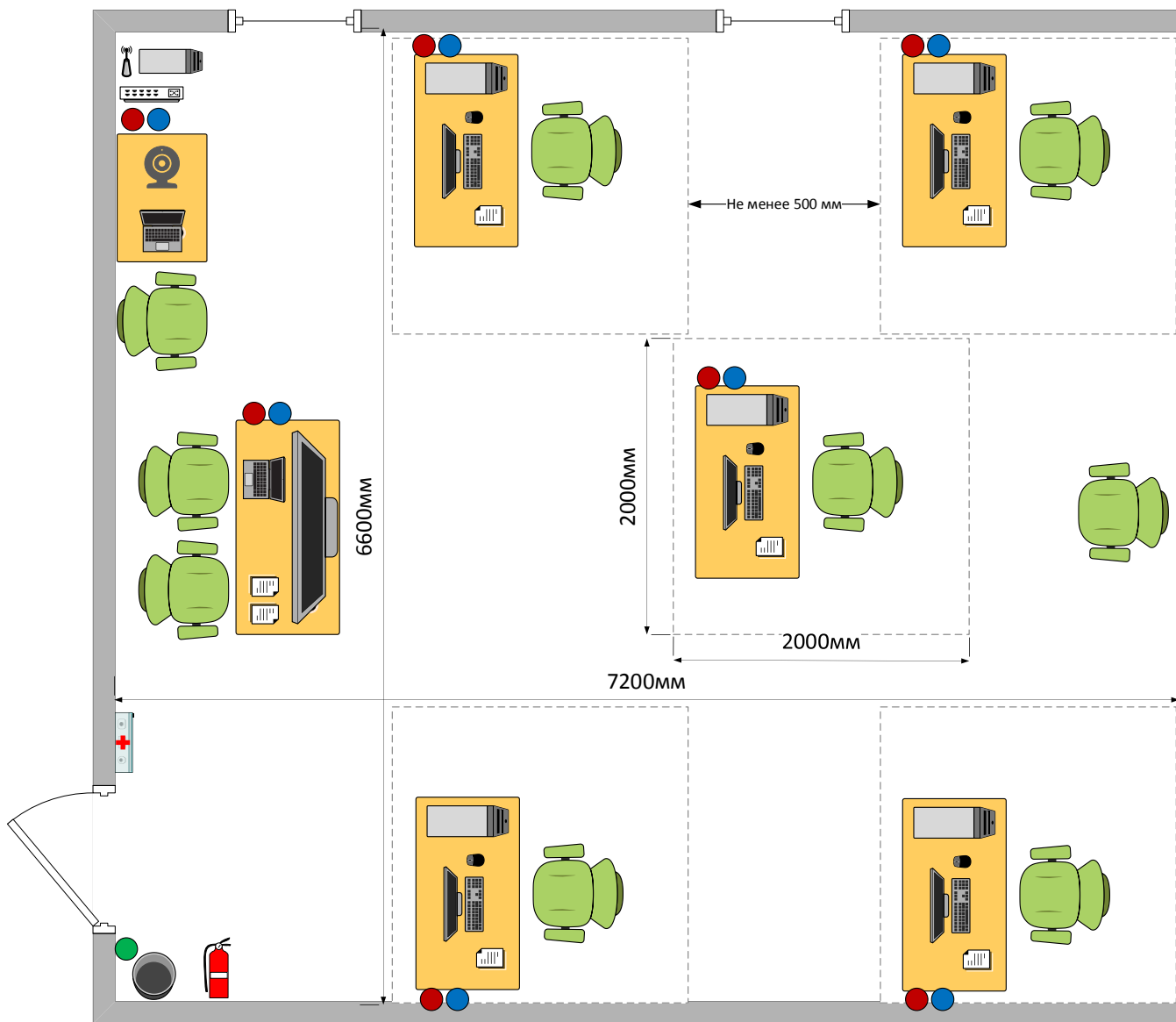
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный)

Формат проведения ДЭ: очный / распределенный

Общая площадь площадки: 80 м²



Площадка проведения экзамена



Образец задания

Образец задания для демонстрационного экзамена по комплекту оценочной документации.

Описание задания

Описание модуля А: Установка, конфигурирование и устранение неисправностей в системы предотвращения вторжений

Введение

В компания «Демо Лаб» возникла необходимость внедрения IDS системы для детектирования (и, при возможности, блокировки) вредоносного внешнего и внутреннего трафика.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы и IP адреса настраиваются согласно заданию.

Подготовлены следующие виртуальные машины для дальнейшей работы:

- Две виртуальные машина для установки IDS,
- Виртуальная машины для установки FTP сервера,
- Центральный Syslog-сервер. (В карточке прописан IP и порт для настройки подключения
- Виртуальная машины для установки системы SIEM систем
- Виртуальные машины с защищаемыми системами

Для большей сетевой безопасности в компании все устройства должны иметь статический IP-адрес. Сетевые настройки указаны в дополнительных сведениях к заданию.

При выполнении заданий можно пользоваться справочными ресурсами в сети Интернет и документацией на компьютерах в общем сетевом каталоге.

Все дистрибутивы находятся в каталоге, указанном в дополнительной карточке задания. Все логины, пароли, сетевые настройки и прочее указаны в дополнительной карточке задания либо в самом задании

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например: Модуль 1_Задание_5_копирование.jpg, все скриншоты и отчеты сохраняются на рабочий стол физического компьютера или передаются экспертам иным способом по запросу.

Задание 1. Начальная установка и настройка системы IDS.

Образ системы IDS развернуть.

1. Использовать сетевой интерфейс для управления и для перехвата трафика

2. Настроить подсеть как дополнительную подсеть для настройки внутренних сервисов.

Использовать адрес как дополнительный интерфейс в IDS

3. Настроить нового администратора системы с полным доступом.

4. Настроить сетевые интерфейсы управления и перехвата, используя карточку доп. сведений.

Зафиксировать выполнение задания скриншотами: настройка виртуальной среды, настройка сетей и пользователей.

Задание 2. Подключение экспорта событий IDS в SYSLOG Server

1. Настроить и запустить модуль IDS.

2. Настроить экспорт событий из IDS в центральный Syslog Server

3. Загрузить на IDS тестовое правило

4. Загрузить дополнительные правила IDS предоставленные производителем

5. После готовности системы на виртуальные машины IDS будет отправлен тестовый трафик для проверки экспорта событий в Syslog Server

Зафиксировать выполнение задания скриншотами: правила и обнаруженные события в IDS, регистрация событий в syslog-сервере.

Задание 3. Подключение экспорта событий IDS в SIEM

1. Образ SIEM развернуть в гипервизоре.

- a. Использовать 1 сетевой интерфейс для управления

- b. Установить IP для интерфейса управления системой SIEM

- c. Настроить нового администратора системы с полным доступом.

- d. Настроить экспорт событий из IDS в SIEM

2. Провести генерацию вредоносного трафика через IDS

3. Проверить, что события экспортировались в систему SIEM

Зафиксировать выполнение задания скриншотами: обнаруженные события в SIEM, установка нового пользователя.

Задание 4. Настройки режима экспорта конфигурации IDS

Задача настроить регулярный экспорт текущей конфигурации IDS на сервер FTP.

1. Установить и настроить сервер FTP сервер в виртуальной машине
2. На FTP сервере настроить пользователя с паролем
3. Настроить сетевой адаптер в виртуальном интерфейсе
4. Настроить подключение IDS к FTP серверу.
5. Настройки расписания экспорта конфигурации каждые N минут.
6. Протестировать режим экспорта методом изменения текущей временной зоны.

Зафиксировать выполнение задания скриншотами: настройка сети, настройка пользователя FTP сервера, настройка сервисов FTP, настройка параметров экспорта, демонстрация экспортированного файла конфигурации.

Задание 5. Настройки режима отказоустойчивого кластера IDS

Задача настроить две системы IDS в режиме кластера на основе двух сетей. будет использоваться для внутренней сети, а заданная администратор сеть будет использоваться для маршрутизации трафика в Интернет. Все интерфейсы должны иметь выделенный IP-адрес, который будет объединен с одним общим виртуальным IP-адресом для связи с обеими сетями.

1. Установить и настроить интерфейсы и основные правила межсетевых экранов.
2. Настроить виртуальные IP-адреса.
3. Настроить синхронизацию
4. Протестировать режим синхронизации через просмотр таблиц состояний.

Зафиксировать выполнение задания скриншотами: настройка сетей, настройка параметров синхронизации, демонстрация таблиц состояний.

Описание модуля F: Предотвращение инцидентов и управление событиями информационной безопасности

После установки и настройки основных систем обнаружения вторжений необходимо проанализировать существующий в сети трафик и создать правило детектирования потенциальных угроз.

Все действия выполняются на системах IDS, настроенных в модуле 1.

Созданные во время выполнения задания правила необходимо называть в формате: mod_1_task_3_rule_1.[формат вашей IDS], все правила сохраняются на рабочий стол.

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например: Модуль_2_Задание_5_копирование.jpg, все скриншоты и отчеты сохраняются на рабочий стол физического компьютера или передаются экспертам иным способом по запросу.

Задание 1. Выявление атаки на веб-сервер с поддержкой PHP

Известно, что на сервер Nginx была проведена попытка использования уязвимости, позволяющей удаленное выполнение произвольного кода, при помощи эксплуатации уязвимости в PHP.

1. Выявить и определить неизвестную атаку методом фильтрации событий, по ключевым словам.
2. Зафиксировать детектирование атаки с помощью IDS в разделе детектированных событий (обязательно с сохранением скриншотов)
3. Зафиксируйте последовательность действий атаки с помощью системы IDS, определите CVE-номер использованной уязвимости, подготовьте отчет об обнаруженной атаке согласно шаблону.

Задание 2. Выявление атаки по протоколу SMB

Задание на выявление угрозы атаки и расследование самой атаки на протокол SMB. Происходит взаимодействие по протоколу SMB для Samba-сервера уязвимой версии. Задача - определить возможную опасность и её последствия с помощью системы IDS.

1. Выявить и определить неизвестную атаку на протокол SMB методом фильтрации событий, по ключевым словам, и использованным портам данного протокола.
2. Зафиксировать детектирование атаки с помощью IDS в разделе детектированных событий (обязательно с сохранением скриншотов)
3. Изучить вредоносную активность и составить детальный план атаки с выявлением нарушителя и определением потенциальных возможностей его скрипта.
4. Определите CVE-номер использованной уязвимости, подготовьте отчет об обнаруженной атаке согласно шаблону.

Задание 3. Выявление атаки на сервис FTP

На сервере с размещённым на нём веб-сервисом может быть получено удаленное выполнение произвольного кода при помощи эксплуатации уязвимости (cve). Для реализации атаки, команды копирования выполняются с правами службы, которая по умолчанию запускается с правами пользователя «nobody». Использование /proc/self/cmdline для копирования полезной нагрузки PHP в каталог веб-сайта делает возможным удаленное выполнение кода PHP.

1. Напишите правило для детектирования всех попыток копирования файлов с расширением “.php” через данный сервис.
2. Проведите проверку собственного правила.
3. Зафиксируйте детектирование атаки с помощью IDS в разделе детектированных событий (обязательно с сохранением скриншотов).

Задание 4. DOS HTTP

Злоумышленники осуществляют DOS атаку http сервера в домашней сети на стандартные порты по установленным соединениям. Нормализованный http пакет содержит некую последовательность.

1. Напишите правило, которое позволяет оповещать пользователя о такого рода атаках.
2. Проведите проверку собственного правила.
3. Зафиксируйте детектирование атаки с помощью IDS в разделе детектированных событий (обязательно с сохранением скриншотов).

Задание 5. Ознакомление с возможной атакой по протоколу Modbus.

Атаки на объекты промышленного комплекса зачастую связаны с эксплуатацией уязвимости протокола modbus (TCP). Сетевой администратор заметил странный трафик, приходящий на порт устройства. Серия запросов, каждый из которых имел номер транзакции «1» и номер функции N, приходили по очереди. Каждый следующий запрос отличался от предыдущего.

1. Определите характер действий злоумышленника?
2. Напишите правило для системы IDS, которое позволяет оповещать администратора о подобном трафике.
3. Проведите проверку собственного правила.
4. Зафиксируйте детектирование атаки с помощью IDS в разделе детектированных событий (обязательно с сохранением скриншотов).

Задание 6. Ознакомление с возможной атакой по протоколу Modbus.

Атаки на объекты промышленного комплекса зачастую связаны с эксплуатацией уязвимости протокола modbus (TCP). Сетевой администратор заметил странный трафик, приходящий на порт устройства. Серия запросов, каждый из которых имел номер транзакции «НОМЕР», записала что-то в регистры устройства.

1. Опишите в отчете характер атаки и насколько критично произошедшее в общем случае?
2. Напишите правило, которое блокирует пакеты с номером транзакции 0 и функциями записи.
3. Проведите проверку собственного правила.
4. Зафиксируйте детектирование атаки с помощью IDS в разделе детектированных событий (обязательно с сохранением скриншотов).

Задание 7. Эксплуатация протокола

Устройство злоумышленника осуществляет проверку захваченных устройств для осуществления DoS атаки. Известно, что входящий ответ имеет идентификатор 123 и содержит слово «СЛОВО».

1. Напишите правило, которое позволяет оповещать пользователя о такого рода атаках.
2. Проведите проверку собственного правила.
3. Зафиксируйте детектирование атаки с помощью IDS в разделе детектированных событий (обязательно с сохранением скриншотов).

Задание 8. Легальный трафик

Доверенный удаленный сервер с известной доверенной сети раз в несколько часов отправляет запрос «ЗАПРОС» со случайных портов, находящихся в промежутке [1; 10].

1. Напишите правило, которое детектирует на IDS прочие поступающие пакеты, содержащие указанный запрос.
2. Проведите проверку собственного правила.
3. Зафиксируйте детектирование атаки с помощью IDS в разделе детектированных событий (обязательно с сохранением скриншотов).

Задание 9. Эксплуатация уязвимости

Было высказано предположение, что если в http заголовке есть функция «ФУНКЦИЯ», то это потенциальная sql-инъекция. Сделайте правило, в котором

проверяется содержимое заголовка на наличие функции «ФУНКЦИЯ» и наличие строки «СТРОКА».

1. Напишите правило, которое позволяет оповещать пользователя о такого рода атаках.
2. Проведите проверку собственного правила.
3. Зафиксируйте детектирование атаки с помощью IDS в разделе детектированных событий (обязательно с сохранением скриншотов).

Описание модуля Е: Технологии защиты узла и агентский мониторинг

Задания выполняются только с помощью групповых политик. Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух и более скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы).

Групповая политика 1

Настроить политику паролей и блокировки:

- Максимальный срок действия пароля
- Минимальная длина пароля
- Блокировка пользователя при неправильном вводе пароля
- Блокировка учетной записи

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Запретить запуск приложений.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

Запретить использование компонентов системы пользователем.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю пользоваться контекстным меню/панелью управления и т. д.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

Изменить изображение рабочего стола пользователя групповыми политиками в домене.

Изменение изображения вручную не будет считаться корректным выполнением задания.

Зафиксировать настройки политики и выполнение скриншотами.

Необходимые приложения

Приложение 1: Карточка настроек сети и оборудования (docx)

Приложение 2. Шаблон отчета об инциденте для неизвестных атак (docx)

7. Комплект оценочной документации паспорт КОД 2.1– 2022

Паспорт комплекта оценочной документации

1. Описание

Комплект оценочной документации (КОД) разработан в целях организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия.

В данном разделе указаны основные характеристики КОД и должны использоваться при планировании, проведении и оценки результатов демонстрационного экзамена образовательными организациями, ЦПДЭ и Агентством.

Таблица 1. Паспорт комплекта оценочной документации (КОД)

№ п/п	Наименование	Информация о разработанном КОД
1	2	3
1	Номер компетенции	F7
2	Название компетенции	Корпоративная защита от внутренних угроз информационной безопасности
3	КОД является однодневным или двухдневным:	Двухдневный
4	Номер КОД	КОД 2.1
4.1	Год(ы) действия КОД	2022 (1 год)
5	Уровень ДЭ	ФГОС СПО
6	Общее максимально возможное количество баллов задания по всем критериям оценки	84,00
7	Длительность выполнения экзаменационного задания данного КОД	11:30:00
8	КОД разработан на основе	ФНЧ Молодые профессионалы 2021
9	КОД подходит для проведения демонстрационного экзамена в качестве процедуры Независимой оценки квалификации (НОК)	НЕТ
10	Вид аттестации, для которой подходит данный КОД	ГИА
11	Формат проведения ДЭ	X
11.1	КОД разработан для проведения ДЭ в очном формате, (участники и эксперты находятся в ЦПДЭ)	Да
11.2	КОД разработан для проведения ДЭ в дистанционном формате, (участники и эксперты работают удаленно)	Да
11.3	КОД разработан для проведения ДЭ в распределенном формате, (детализация в п.11.3.1)	Да
11.3.1	Формат работы в распределенном формате	Участники находятся в ЦПДЭ, эксперты работают удаленно
12	Форма участия (индивидуальная, парная, групповая)	Индивидуальная

12.1	Количество человек в группе, (т.е. задание ДЭ выполняется индивидуально или в группе/ команде из нескольких экзаменуемых)	1,00
12.2	Организация работы при невозможности разбить экзаменуемых на указанное в п. 12.1 количество человек в группе	
13	Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3,00
16	Автоматизированная оценка результатов заданий	Частичная автоматизация
16.1	Что автоматизировано: заполняется при выборе вариантов в п.16: возможна частичная или полная автоматизация	Модуль 3 (в зависимости от возможностей площадки)

2. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта

Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта, (WorldSkills Standards Specification WSSS), проверяемый в рамках комплекта оценочной документации, (Таблица 2).

Таблица 2. WSSS

Номер раздела WSSS	Наименование раздела WSSS	Содержание раздела WSSS: Специалист должен знать	Важность раздела WSSS (%)
1	2	3	4

2	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	<p>Специалист должен знать и понимать:</p> <p>Сетевое окружение; Сетевые протоколы; Знать методы выявления и построения путей движения информации в организации; Подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия; Типы сетевых устройств; Разнообразии операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз; Процесс выбора подходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем; Важность следования инструкциям и последствия, цену пренебрежения ими; Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы; Этапы установки системы корпоративной защиты от внутренних угроз; Знать отличия различных версий систем корпоративной защиты от внутренних угроз; Знать какие СУБД поддерживаются системой; Знать назначение различных компонент версий систем корпоративной защиты от внутренних угроз; Знать технологии программной и аппаратной виртуализации; Знать особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation; Цель документирования процессов обновления и установки. Важность спокойного и сфокусированного подхода к решению проблемы; Значимость систем ИТ-безопасности и зависимость пользователей и организаций от их доступности; Популярные аппаратные и программные ошибки; Знать разделы системы корпоративной безопасности, которые обычно использует системный администратор; Аналитический и диагностический подходы к решению проблем; Границы собственных знаний, навыков и полномочий; Ситуации, требующие вмешательства службы поддержки; Стандартное время решения наиболее популярных проблем. Специалист должен уметь: Интерпретировать пользовательские запросы и требования с точки зрения корпоративных требований;</p>	30
---	---	--	----

		<p>Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении; Настраивать сетевые устройства; Администрирование автоматизированных технических средства управления и контроля информации и информационных потоков; Навыки системного администрирования в операционных системах Windows, Windows Server, Linux (Red Hat Enterprise Linux, CentOS и др.); Навыки системного администрирования в защищенных операционных системах (AstraLinux и др.); Настройка в операционных системах прав доступа в соответствие с ролевой и/или мандатной моделью; Настройка средств виртуализации под операционными системам; Конфигурирование операционных систем для правильного и защищенного использования средств безопасности, в т.ч. системы корпоративной защиты от внутренних угроз.; Установка серверной части системы корпоративной защиты от внутренних угроз; Установка СУБД различного вида; Установка агентской части системы корпоративной защиты от внутренних угроз; Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом; Использовать дополнительные утилиты если это необходимо; Уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки; Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае необходимости; Уметь сконфигурировать систему, чтобы она получала теневые копии; Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах; Демонстрировать уверенность и упорство в решении проблем; Быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы, точно описывать проблему и документировать её решение; Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей; Выбирать и принимать диагностирующее ПО и инструменты для поиска неисправностей;</p>	
--	--	---	--

4	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	<p>Специалист должен знать и понимать:</p> <p>Технологии работы с политиками информационной безопасности;</p> <p>Создание новых политик, модификация существующих;</p> <p>Общие принципы при работе интерфейсом системы защиты корпоративной информации;</p> <p>Объекты защиты, персоны;</p> <p>Ключевые технологии анализа трафика;</p> <p>Типовые протоколы и потоки данных в корпоративной среде, такими как: корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4) веб-почта;</p> <p>Интернет-ресурсы: сайты, блоги, форумы и т.д. (протоколы HTTP, HTTPS); социальные сети;</p> <p>интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP;</p> <p>принтеры: печать файлов на локальных и сетевых принтерах;</p> <p>любые съемные носители и устройства;</p> <p>Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек;</p> <p>Типы угроз информационной безопасности, типы инцидентов,</p> <p>Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;</p> <p>Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации;</p> <p>Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;</p> <p>Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации;</p> <p>Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки;</p> <p>Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе;</p> <p>Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов;</p> <p>Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации;</p> <p>Специалист должен уметь:</p> <p>Создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты;</p>	18,00
---	---	--	-------

		<p>Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты;</p> <p>Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии;</p> <p>Работа со сводками, виджетами, сводками;</p> <p>Работа с персонami;</p> <p>Работа с объектами защиты;</p> <p>Провести имитацию процесса утечки конфиденциальной информации в системе;</p> <p>Создать непротиворечивые политики, соответствующие нормативной базе и законодательству;</p> <p>Задokumentировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации.</p> <p>Работа с категориями и терминами;</p> <p>Использование регулярных выражений;</p> <p>Использование морфологического поиска;</p> <p>Работа с графическими объектами;</p> <p>Работа с выгрузками и баз данных;</p> <p>Работа с печатями и бланками;</p> <p>Работа с файловыми типами;</p> <p>Эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;</p>	
5	Технологии защиты и анализа сетевого трафика	<p>Специалист должен знать и понимать:</p> <p>Организационно-технические и правовые основы использования электронного документооборота в информационных системах;</p> <p>Структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей;</p> <p>Нормативно-правовые документы, требования законодательства и регулирующих органов РФ в области электронной подписи, удостоверяющих центров, СКЗИ, МЭ;</p> <p>Классы защищенности и уровни доверия СЗИ;</p> <p>Технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений;</p> <p>Ключевые компоненты VPN-сетей;</p> <p>Особенности VPN-сети и механизмы их управления;</p> <p>Современные криптографические алгоритмы. Криптопровайдеры, криптографические интерфейсы и библиотеки;</p> <p>Архитектура, основные компоненты PKI их функции и взаимодействие;</p> <p>Назначение и роль доверенного удостоверяющего центра в системе ключевой</p>	14,00

		<p>инфраструктуры организации; Жизненный цикл ключей и сертификатов; Электронный сертификат ключей ЭП. Формирование, подписание и использование сертификатов; Защита видео и конференций приложений; Назначение и основные сценарии применения IDS-технологий; Архитектуру и особенности внедрения IDS-технологий; Распространённые вектора атак и уязвимости современных корпоративных информационных систем. Специалист должен уметь: Осуществлять развёртывание и администрирование VPN-сетью (добавление, удаление, изменение объектов сети, настройка параметров работы, контроль работоспособности и др.). Обновление ПО, установленного на узлах защищенной сети. Работать и удостоверяющей и ключевой информацией. Формирование и управление ключевой структурой сети. Издание и управление сертификатами пользователей. Настраивать защиту сегментов IP-сетей, координация работы узлов защищенной сети. Защиты трафика, передаваемого по открытым каналам связи; Осуществлять защиту оконечных рабочих мест; Контроль пользовательских приложений; Реализовывать межсетевое взаимодействие и туннелирование; Компрометация рабочих мест; Обеспечение межсетевого экранирования и криптографической защиты информации; Производить установку, настройку, развёртывание удостоверяющих центров инфраструктуры открытых ключей включая подсистемы регистрации пользователей, создания ключей ЭП, издания сертификатов ключей проверки ЭП, поддержания инфраструктуры ключей проверки ЭП. Конфигурировать ПО для электронного документооборота в VPN-системах; Защита систем, обеспечивающих поддержку процессов информационного взаимодействия; Выполнять настройку и проверку работоспособности; Проводить детектирование атак (потенциальных угроз) в ручном, автоматизированном и автоматическом режиме; Проводить правильную классификацию уровня угрозы инцидента; Использовать базы контентной фильтрации; Использовать дополнительные модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса;</p>	
--	--	---	--

6	Технологии защиты узла и агентского мониторинга	<p>Специалист должен знать и понимать: Функции агентского мониторинга; Общие настройки системы агентского мониторинга; Соединение с LDAP-сервером и синхронизация с Active Directory; Политики агентского мониторинга, особенности их настройки; Особенности настроек событий агентского мониторинга; Механизмы диагностики агента, подходы к защите агента. Знать возможности и ограничения современных российских и зарубежных операционных систем в рамках решения задач защиты информации Знать архитектуру операционных систем Знать инструментарий по работа с современными операционными системами, команды, ПО, утилиты Специалист должен уметь: Установка и настройка агентского мониторинга; Создание политик защиты на агентах; Работа в консоли управления агентом; Фильтрация событий; Настройка совместных событий агентского и сетевого мониторинга; Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата. Производить настройку сервисов и компонент операционной системы для достижения целей защиты Разделять компоненты операционной системы по уровням доверия, сокращая поверхность атаки для злоумышленника Применять механизмы ролевого и мандатного доступа и контроля целостности Реализовывать ограниченную программную среду для пользователя Знать особенности безопасной работы и загрузки операционных систем на различных аппаратных платформах</p>	18,00
7	Предотвращение инцидентов и управление событиями информационной безопасности	<p>Специалист должен знать и понимать: Назначение, роль, возможности систем IDS/IPS для задачи защиты организации от угроз информационной безопасности Назначение, роль, возможности систем SIEM для задачи защиты организации от угроз информационной безопасности Назначение, роль, возможности систем Threat Intelligence для задачи защиты организации от угроз информационной безопасности Специалист должен уметь: Устанавливать, настраивать системы IDS/IPS</p>	4,00

		Устанавливать, настраивать системы SIEM Устанавливать, настраивать системы Threat Intelligence, генерации трафика и проверки защищенности Применять на практике системы IDS/IPS для выявления инцидентов информационной безопасности Применять на практике системы Threat Intelligence Применять на практике системы Threat Intelligence и Attack Simulation (Breach and Attack Simulation) для проверки/оценки устойчивости систем и сетей к компьютерным атакам Проводить анализ выявленных инцидентов, использовать встроенные и внешние системы подготовки отчетности	
--	--	--	--

*Таблица соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами

доступна

в

Приложении

3. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке

Минимальное количество линейных экспертов, участвующих в оценке демонстрационного экзамена по компетенции	3
---	---

Соотношение количества экспертов в зависимости от количества экзаменуемых и количества рабочих мест.

Таблица 3. Расчет количества экспертов исходя из количества рабочих мест и участников.

Количество постов-рабочих мест на экзаменационной площадке	Количество участников <u>на одно пост-рабочее</u> место на одной экзаменационной площадке (по умолчанию 1 участник)	Максимальное количество участников в одной экзаменационной группе одной экзаменационной площадки	Количество экспертов на одну экзаменационную группу одной экзаменационной площадки
1	2	3	4
1	1	1	3
2	1	2	3
3	1	3	3
4	1	4	3
5	1	5	3
6	1	6	3
7	1	7	3
8	1	8	3
9	1	9	3
10	1	10	3
11	1	11	3
12	1	12	3
13	1	13	4
14	1	14	4
15	1	15	4
16	1	16	4
17	1	17	4
18	1	18	4
19	1	19	4
20	1	20	4
21	1	21	5
22	1	22	5
23	1	23	5
24	1	24	5
25	1	25	5

4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

По результатам выполнения заданий демонстрационного экзамена может быть применена схема перевода баллов из стобалльной шкалы в оценки по пятибалльной шкале.

Таблица 4. Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную

Оценка	«2»	«3»	«4»	«5»
1	2	3	4	5
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00% - 19,99%	20,00% - 39,99%	40,00% - 69,99%	70,00% - 100,00%

5. Список оборудования и материалов, запрещенных на площадке (при наличии)

Таблица 5. Список оборудования и материалов, запрещенных на площадке, (при наличии)

№ п/п	Наименование запрещенного оборудования
1	2
1	Личный мобильный телефон (смартфон)
2	Наушники с передачей аудио (проводные, беспроводные)
3	Личный ноутбук
4	Личный планшет
5	Личная клавиатура
6	Личная компьютерная мышь

6. Детальная информация о распределении баллов и формате оценки.

Таблица 6. Обобщенная оценочная ведомость.

№ п/п	Модуль задания, где проверяется критерий	Критерий	Длительность модуля	Разделы WSSS	Судейские баллы	Объективные баллы	Общие баллы
1	2	3	4	5	6	7	8
1	А: Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	1:30:00	2,5	0,00	14,00	14,00
2	Е: Технологии защиты узла и агентского мониторинга	Технологии защиты узла и агентского мониторинга	2:00:00	6	0,00	18,00	18,00
3	С: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	2:00:00	4	0,00	18,00	18,00
4	Ф: Предотвращение инцидентов и управление событиями информационной безопасности	Предотвращение инцидентов и управление событиями информационной безопасности	0:30:00	7	0,00	4,00	4,00
5	А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	3:00:00	2,5	0,00	16,00	16,00
6	Д: Технологии защиты и анализа сетевого трафика	Технологии защиты и анализа сетевого трафика	2:30:00	2,5	0,00	14,00	14,00
Итого	-	-	11:30:00	-	0,00	84,00	84,00

7. Примерный план работы Центра проведения демонстрационного экзамена⁶.

Таблица 7. Примерный план работы Центра проведения демонстрационного экзамена.

День (выберете из выпадающего списка)	Начало мероприяти я (укажите в формате ЧЧ:ММ)	Окончание мероприяти я (укажите в формате ЧЧ:ММ)	Длительность мероприятия (расчет производится автоматически)	Мероприятие	Действия экспертной группы при распределенном формате ДЭ (Заполняется при выборе распределенного формата ДЭ)	Действия экзаменуемых при распределенно м формате ДЭ (Заполняется при выборе распределенног о формата ДЭ)	Действия экспертной группы при дистанционном формате ДЭ (Заполняется при выборе дистанционного формата ДЭ)	Действия экзаменуемых при дистанционно м формате ДЭ (Заполняется при выборе дистанционног о формата ДЭ)
1	2	3	4	5	6	7	8	9
Подготовительны й день (С-1)	09:00:00	09:15	0:15:00	Получение главным экспертом задания демонстрационног о экзамена	—	—	—	—
Подготовительны й день (С-1)	09:15:00	10:00:00	0:45:00	Проверка готовности проведения демонстрационног о экзамена, заполнение Акта о готовности площадки	Проверка подключения к площадке, сверка участников	—	Проверка подключения к площадке, сверка участников	—

⁶ Если планируется проведение демонстрационного экзамена для двух и более экзаменационных групп (ЭГ) из одной учебной группы одновременно на одной площадке, то это также должно быть отражено в плане. Примерный план рекомендуется составить таким образом, чтобы продолжительность работы экспертов на площадке не превышала нормы, установленные действующим законодательством. В случае необходимости превышения установленной продолжительности по объективным причинам, требуется согласование с экспертами, задействованными для работы на соответствующей площадке.

Подготовительный день (С-1)	10:00:00	10:15:00	0:15:00	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение протоколов	Заполнение протоколов онлайн	—	Заполнение протоколов онлайн	—
Подготовительный день (С-1)	10:15:00	10:30:00	0:15:00	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Проверка подключения к площадке	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Проверка подключения к площадке
Подготовительный день (С-1)	10:30:00	10:45:00	0:15:00	Регистрация участников демонстрационного экзамена	Контроль за регистрацией	Регистрация с помощью веб-камеры (мобильного телефона или иного устройства)	Контроль за регистрацией	Регистрация с помощью веб-камеры (мобильного телефона или иного устройства)
Подготовительный день (С-1)	10:45:00	11:15:00	0:30:00	Инструктаж участников по охране труда и технике безопасности, сбор подписей в протоколах	Контроль за протоколами	Инструктаж по ОТиТБ, заполнение протоколов онлайн	Контроль за протоколами	Инструктаж по ОТиТБ, заполнение протоколов онлайн

Подготовительный день (С-1)	11:15:00	13:00:00	1:45:00	Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение протоколов	Контроль за протоколами, жеребьевкой	Жеребьевка, проверка подключения к рабочим местам, заполнение протоколов онлайн	Контроль за протоколами, жеребьевкой	Жеребьевка, проверка подключения к рабочим местам, заполнение протоколов онлайн
Подготовительный день (С-1)	13:00:00	16:00:00	3:00:00	Подготовка и/или проверка работоспособности и площадки в соответствии с заданием	Проверка работоспособности и площадки, помощь ГЭ (при необходимости), Завершение дня	Завершение дня	Проверка работоспособности и площадки, помощь ГЭ (при необходимости), Завершение дня	Завершение дня
День 1	08:45:00	09:00:00	0:15:00	Ознакомление с заданием и правилами	Подключение к площадке и системе ВКС, контроль за подключением участников	Подключение к площадке и системе ВКС, получение задания, ознакомление	Подключение к площадке и системе ВКС, контроль за подключением участников	Подключение к площадке и системе ВКС, получение задания, ознакомление
День 1	09:00:00	09:15:00	0:15:00	Брифинг		Ознакомление с заданием, вопросы		Ознакомление с заданием, вопросы
День 1	09:15:00	10:45:00	1:30:00	Выполнение модуля А	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ

День 1	10:45:00	11:00:00	0:15:00	Перерыв, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 1	11:00:00	13:00:00	2:00:00	Выполнение модуля Е	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 1	13:00:00	13:45:00	0:45:00	Обед, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 1	13:45:00	15:45:00	2:00:00	Выполнение модуля С	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 1	15:45:00	16:00:00	0:15:00	Перерыв, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 1	16:00:00	16:30:00	0:30:00	Выполнение модуля F	Контроль за участниками и выполнением работ	Выполнение работ, завершение работы	Контроль за участниками и выполнением работ	Выполнение работ, завершение работы
День 1	16:30:00	18:30:00	2:00:00	Работа экспертов, заполнение форм и оценочных ведомостей	Оценка работ с помощью средств удаленного управления (подключения к площадке), проставление баллов	—	Оценка работ с помощью средств удаленного управления (подключения к площадке), проставление баллов	—

День 1	18:30:00	19:30:00	1:00:00	Подведение итогов, внесение главным экспертом баллов в CIS, сверка баллов	Внесение баллов в CIS	—	Внесение баллов в CIS	—
День 2	08:45:00	09:00:00	0:15:00	Ознакомление с заданием и правилами	Подключение к площадке и системе ВКС, контроль за подключением участников	Подключение к площадке и системе ВКС, получение задания, ознакомление	Подключение к площадке и системе ВКС, контроль за подключением участников	Подключение к площадке и системе ВКС, получение задания, ознакомление
День 2	09:00:00	09:15:00	0:15:00	Брифинг		Ознакомление с заданием, вопросы		Ознакомление с заданием, вопросы
День 2	09:15:00	10:45:00	1:30:00	Выполнение модуля А	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 2	10:45:00	11:00:00	0:15:00	Перерыв, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 2	11:00:00	12:30:00	1:30:00	Выполнение модуля А	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 2	12:30:00	13:15:00	0:45:00	Обед, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв

День 2	13:15:00	14:30:00	1:15:00	Выполнение модуля D	Контроль за участниками и выполнением работ	Выполнение работ	Контроль за участниками и выполнением работ	Выполнение работ
День 2	14:30:00	14:45:00	0:15:00	Перерыв, обработка помещения, проветривание	Перерыв	Перерыв	Перерыв	Перерыв
День 2	14:45:00	16:00:00	1:15:00	Выполнение модуля D	Контроль за участниками и выполнением работ	Выполнение работ, завершение работы	Контроль за участниками и выполнением работ	Выполнение работ, завершение работы
День 2	16:00:00	18:00:00	2:00:00	Работа экспертов, заполнение форм и оценочных ведомостей	Оценка работ с помощью средств удаленного управления (подключения к площадке), проставление баллов	—	Оценка работ с помощью средств удаленного управления (подключения к площадке), проставление баллов	—
День 2	18:00:00	19:00:00	1:00:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение протоколов	Внесение баллов в CIS, подписание протокола с использованием ЭП или сканирования (фото) протокола	—	Внесение баллов в CIS, подписание протокола с использованием ЭП или сканирования (фото) протокола	—

8. Необходимые приложения

Приложение 2. Соответствия знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами.

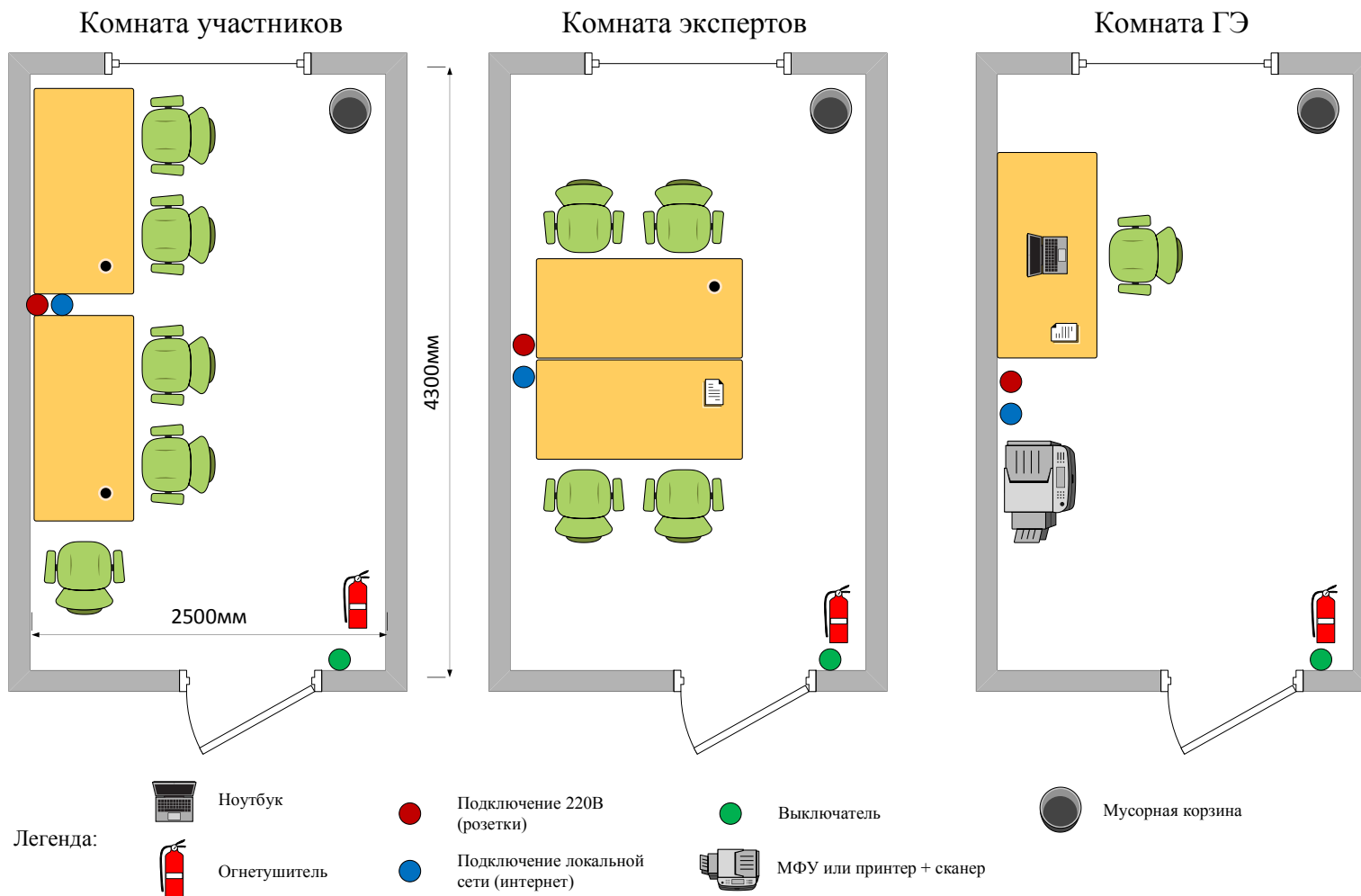
Приложение 5. План застройки площадки для проведения демонстрационного экзамена.

Приложение 6. Инфраструктурный(-ые) лист(-ы).

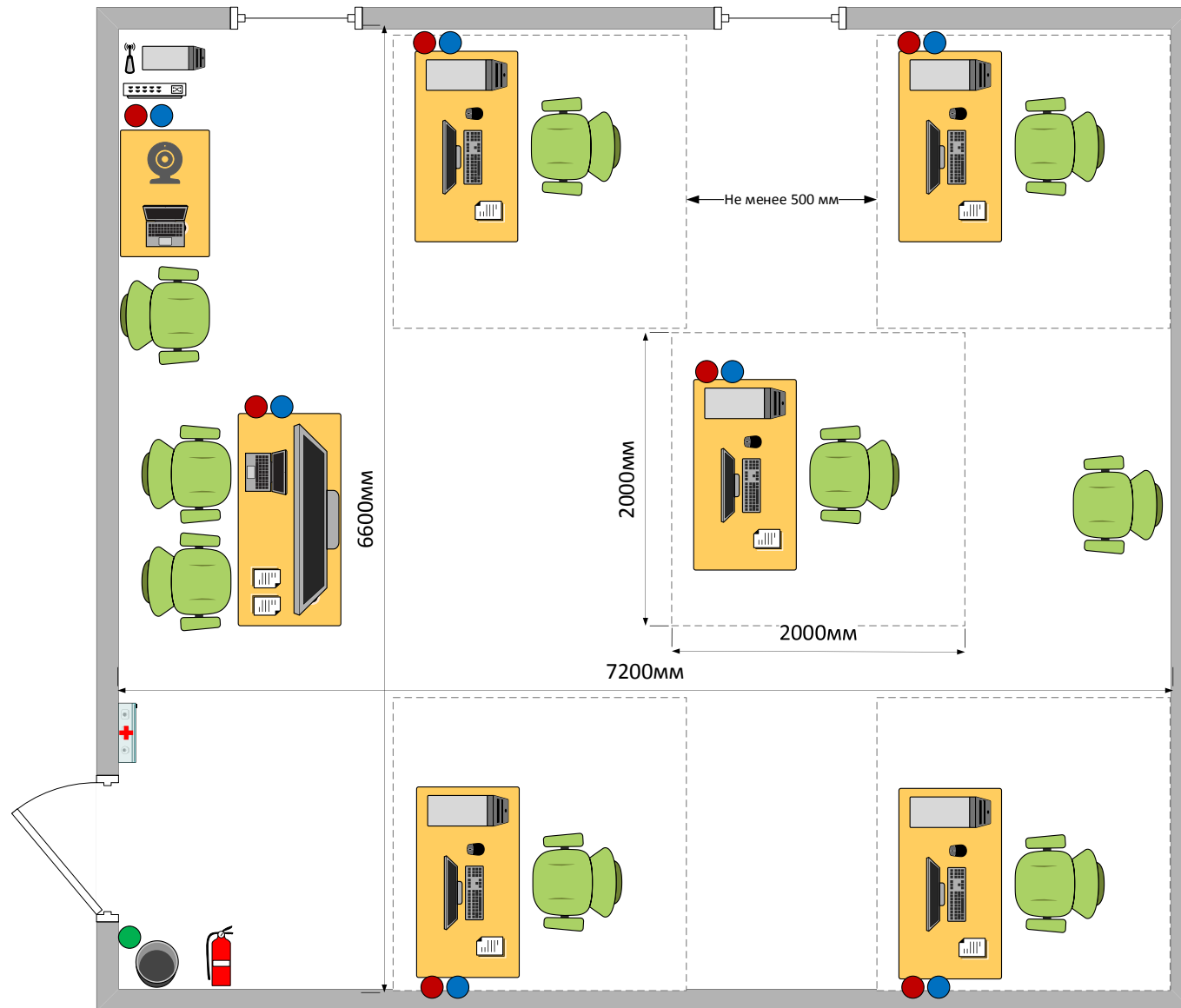
План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (очный / распределенный)

Формат проведения ДЭ: очный / распределенный

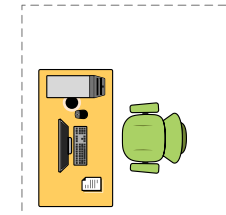
Общая площадь площадки: 80 м²













Площадка проведения экзамена



Легенда



Рабочее место (2×2 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, USB-накопитель, набор ПО

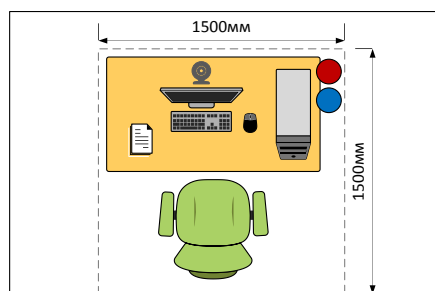
-  Ноутбук
-  Аптечка
-  Огнетушитель
-  ТВ/проектор (таймер)
-  Камера (трансляция)
-  Сетевая инфраструктура (сервер, коммутатор/маршрутизатор, точка доступа), может быть в серверной
-  Подключение 220В (розетки)
-  Подключение локальной сети (интернет)
-  Выключатель
-  Мусорная корзина

План застройки площадки центра проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия (дистанционный)

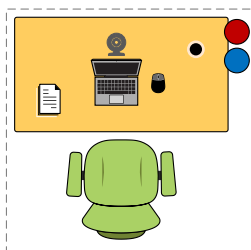
Формат проведения ДЭ: дистанционный

Общая площадь площадки: 2,25 м² (и более, на 1 участника/эксперта)

Рабочее место участника

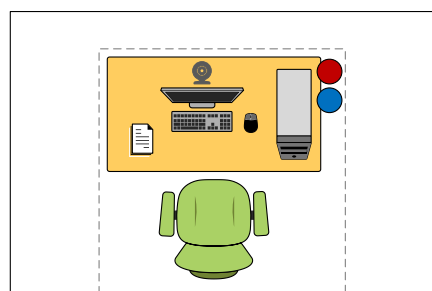


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

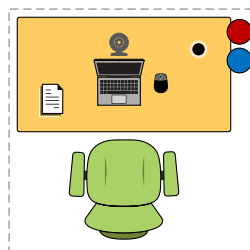


Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

Рабочее место эксперта

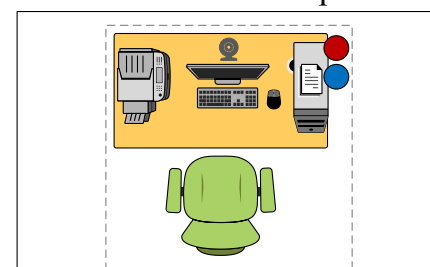


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

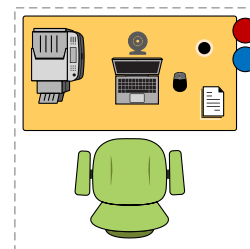


Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, набор ПО, доступ к Интернет (кабель или беспроводной)

Рабочее место главного эксперта

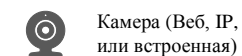


Вариант 1:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, компьютер, монитор, клавиатура, мышь, веб-камера, МФУ (принтер и сканер) или принтер + камера или смартфон (для «сканирования») набор ПО, доступ к Интернет (кабель или беспроводной)



Вариант 2:
Рабочее место (1,5×1,5 м и более) в составе: стол, стул, ноутбук (опционально мышь), веб-камера, МФУ (принтер и сканер) или принтер + камера или смартфон (для «сканирования»), набор ПО, доступ к Интернет (кабель или беспроводной)

Легенда:



Камера (Веб, IP, или встроенная)



Подключение 220В (розетки)



Подключение локальной сети (интернет) или WiFi



МФУ или принтер + сканер, или принтер + камера/ смартфон/ планшет прочее с камерой

Образец задания

Образец задания для демонстрационного экзамена по комплексу оценочной документации.

Описание задания

В компании «Демо Лаб» возникла необходимость внедрения DLP системы для лучшей защиты разработок и предотвращения утечек прочей информации. Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием. Основными каналами потенциальной утечки данных являются электронная почта и различные интернет-ресурсы, если не указано иное.

Политики трафика могут быть проверены вручную или с помощью генератора событий, предоставляемым по запросу.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены (кроме адреса DNS сервера на машинах).

Перед экзаменом должны быть подготовлены следующие виртуальные машины для работы (рекомендуется сделать нулевой Snapshot для быстрой подготовки к другим потокам), сеть настроена в режиме NAT (сеть NAT) или Bridge с DHCP, с доступом в интернет, но без доступа к машинам других участников экзамена:

- AD и DNS сервер (контроллер домена), 1,5ГБ ОЗУ и выше, 2 ядра, статическая адресация с доступом в интернет,
- DLP сервер установлен (но не настроен), активирована лицензия, 6ГБ ОЗУ и выше, 2 ядра,
- Виртуальная машина для установки сервера агентского мониторинга, 2ГБ ОЗУ и выше, 2 ядра,
- Виртуальные машины «нарушителей» (2 шт), 1,5ГБ ОЗУ и выше, 2 ядра.

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов (demo.lab, должен быть развернут из эталонного, получить эталон можно по запросу).

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными. При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и документацией на компьютерах.

Все дистрибутивы должны находиться в каталоге, указанном в карточке задания. Все логины, пароли, сетевые настройки и прочее, относящееся к инфраструктуре площадки, должно быть указано в карточке задания.

При создании снимков экрана необходимо делать либо полный снимок экрана, либо целого окна.

Описание модуля А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Задание 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “Test” в корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

Внутри созданного подразделения “Test” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: user1, пароль: ххХХ1234, права пользователя домена

Логин: user2, пароль: ххХХ1234, права пользователя домена

Логин: admin1, пароль: ххХХ1234, права администратора домена

Логин: user3, пароль: ххХХ1234, права пользователя домена

Логин: user4, пароль: ххХХ1234, права пользователя домена

Задание 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен.

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя user4.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена user3 с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» на рабочем столе компьютера.

Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя admin1 (важно). После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “Test” на домене.

Установить базу данных PostgreSQL или функциональный аналог с паролем суперпользователя ххХХ1234.

Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: `officer` с паролем `xxXX1234`

Синхронизировать каталог пользователей и компьютеров с Active Directory или функциональным аналогом.

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя `admin1`, установить полный доступ к системе, установить все области видимости.

Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.

Задание 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину 1 в домен, после перезагрузки войти в систему от ранее созданного пользователя `user1`.

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя `user2`.

После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение “Test” на домене.

Установить агент мониторинга:

На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга.

На машину 2 с помощью групповых политик домена.

Необходимо создавать отдельные объекты групповых политик на каждое задание и делать снимки экрана для подтверждения создания и выполнения политик.

Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания

Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов.

Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга с настройками по умолчанию.

Необходимо создать общий каталог Test в корне диска сервера и установить права доступа на запись и чтение для всех пользователей домена.

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. Для работы подсистемы может потребоваться редактирования конфигурационных файлов (для устранения предупреждения).

Задание 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих некий термин, установить уровень угрозы для всех событий, добавить тег.

Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя 1 с установленным агентом.

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа, настроив конструктор выборки вручную.

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задание 7: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям, параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать:

4. корневой root-сертификат (ca)
5. серверный (server) сертификат
6. по желанию допускается использование пользовательского и промежуточного сертификата

Поля сертификата заполняются по вариантам заданий.

После генерации сертификатов необходимо установить серверный сертификат на веб-сервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети для доверенного подключения к веб-консоли DLP-системы уровня сети.

Итоговый результат должен включать:

Дерево из 2-3 сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе. Содержимое команд по генерации ключей и сертификатов в текстовом файле на рабочем столе с комментариями.

Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).

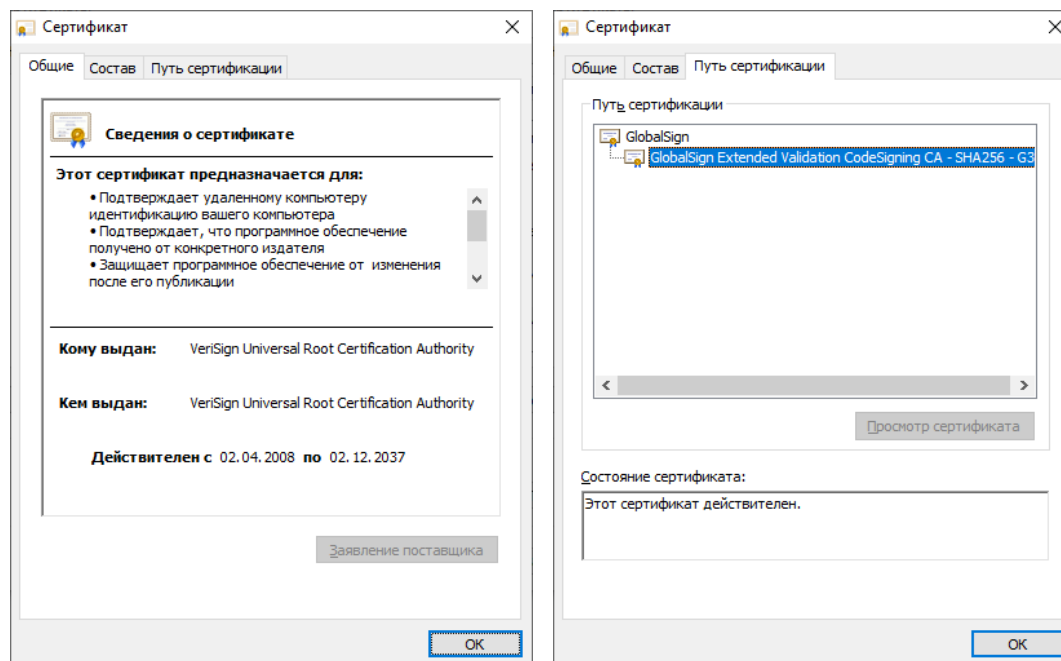


Рис1. Пример скриншотов задания

Описание модуля Е: Технологии защиты узла и агентский мониторинг

Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании). Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна. Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно).

Задание 1

Необходимо создать 2 новых группы компьютеров: «Test1» и «Test2», а также создать 2 новых политики: «Test1» и «Test2». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 необходимо перенести в Test1, а компьютер 2 — в Test2.

Зафиксировать выполнение скриншотом.

Задание 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на другую машину для удаленного доступа к серверу агентского мониторинга.

Следующие правила создаются в политике «Test1».

Правило 1

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 3

Ограничить доступ к определенным облачным хранилищам (по вариантам).

Проверить работоспособность и зафиксировать выполнение

Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Правило 5

Необходимо запретить запись файлов на определенные носители информации, при этом оставить возможность считывания информации.

Проверить работоспособность и зафиксировать выполнение

Правило 6

С учетом ранее созданной блокировки необходимо разрешить использование доверенного носителя информации.

Проверить работоспособность и зафиксировать выполнение

Правило 7

Полностью запретить использование определенного устройства для пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 8

С учетом ранее выполненного запрета необходимо предоставить временный доступ для определенного устройства на определенное время для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Следующие правила создаются в политике «Test2».

Правило 9

Необходимо поставить на контроль буфер обмена в блокноте и notepad++.

Проверить занесение нескольких событий в WEB-консоль.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 10

Необходимо запретить использовать терминальные сессии для пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 11

Необходимо установить контроль за компьютером потенциального нарушителя путем создания снимков экрана каждые 60 секунд или при смене окна.

Проверить работоспособность и зафиксировать выполнение

Правило 12

Запретить передачу файлов определенного типа на съемные носители информации или в сетевое расположение.

Проверить работоспособность и зафиксировать выполнение

Групповые политики домена

Групповые применяются только на компьютер 2, должны быть созданы в домене. Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например запрет запуска).

Групповая политика 1

Настроить политику паролей и блокировки: Максимальный срок действия пароля, Минимальная длина пароля, Сложность пароля, Блокировка учетной записи при неверном вводе пароля.

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Запретить запуск приложений по списку (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

Запретить использование элементов системы стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельно менять параметры системы (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

Настроить дополнительные параметры системы, которые должны применяться для пользователя или компьютера (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Описание модуля С: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям. Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием. После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Для некоторых политик могут понадобиться дополнительные файлы, расположение которых можно узнать из карточки задания или у экспертов.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). Скриншоты необходимо сохранить в папке «Модуль 3».

Скриншоты необходимо называть в соответствии с номером задания и типом задания (Например Политика 2, Задание 1–1 и т. д.)

Задания на разработку политик можно выполнять в любом порядке.

Наиболее сложные политики находятся в конце.

При разработке политик стоит учитывать, что все политики трафика могут передаваться как через веб-сообщения, так и через почтовые сообщения. В случае, если данный пункт не соблюден, то проверка заданий может быть невозможной.

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации.

Список тегов для политик:

Политика 1, Политика 2, Политика 3, ...

Задание 1

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты.

Задание 2

Создайте локальную группу пользователей и добавьте в нее пользователей.

Задание 3

Создать список веб-ресурсов. Добавить в список следующие сайты: Site.ru, domain.com, ...

Задание 4

Для работы системы необходимо настроить периметр компании: Почтовый домен, список веб ресурсов, группа персон, исключить из перехвата.

Политика 1

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела (по вариантам) отправлять документы, содержащие информацию о паспортных данных за пределы компании. Отдел (по вариантам) может отправлять файлы без ограничений.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 1

Политика 2

Для контроля за движением документов необходимо вести наблюдение за передачей шаблона документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах определенного уровня.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 2

Политика 3

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика.

Вердикт: заблокировать

Уровень нарушения: низкий

Тег: Политика 3

Политика 4

Необходимо отслеживать документы, содержащие печать компании всем сотрудникам, кроме отдела (по вариантам) и определенного сотрудника. Они могут обмениваться документами внутри и за пределами компании без контроля.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 4

Политика 5

В последнее время возникла необходимость обработки текстовых данных, а также сканов и фото кредитных карт. Необходимо отслеживать передачу всех возможных данных кредитных карт (в том числе сканов) за пределы компании.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 5

Политика 6

Сотрудники заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из определенного отдела, для остальных контролировать не нужно.

Критичными данными в выгрузке являются определенные поля и в 1 документе присутствует более 1 строчки. Для настройки используйте файл примера.

Вердикт: разрешить
Уровень нарушения: средний
Тег: Политика 6

Политика 7

Некая компания попросила обеспечить защиту от утечки важных данных. Необходимо создать политику на контроль правила передачи содержащие слова «один», «два», «три» в 1 сообщении или документе одновременно. Если в документе встречается только по 1 слову из перечисленных — политика срабатывать не должна.

Правило должно срабатывать на сообщения, которые отправляются за пределы компании всеми пользователями, кроме определенного отдела, который может отсылать информацию свободно.

Вердикт: разрешить
Уровень нарушения: средний
Тег: Политика 7

Политика 8

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании за пределы компании, запрещая любую внешнюю передачу документов в пустых и заполненных бланках.

Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно.

Вердикт: разрешить
Уровень нарушения: средний
Тег: Политика 8

Политика 9

Пользователи стали часто обмениваться ссылками и файлами, в связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов, например формата.mp4 и ссылок определенного формата (содержит уникальную последовательность, например urlname). Ложных срабатываний быть не должно.

Вердикт: Заблокировать
Уровень нарушения: средний
Тег: Политика 9

Политика 10

Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость отследить утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты.

Важно, чтобы в одном сообщении содержалось минимум 2 адреса (т. к. в противном случае будут детектироваться все почтовые сообщения)!

Возможные домены первого уровня: ru, org и прочие. Детектирование только частей адресов (например @mail.ru) недопустимо.

Вердикт: разрешить

Уровень нарушения: высокий

Тег: Политика 10

Политика 11

В связи с разгильдяйством сотрудников, передающих свои пароли коллегам с помощью почты и сообщений, необходимо предотвратить передачу любых стандартизированных паролей для информационной системы в открытом виде любыми отправителями и получателями как внутри, так и за пределы компании.

Стоит учесть, что пароли могут передаваться любым указанным способом: социальные сети и прочие ресурсы (в браузере), мессенджеры, почта, флешки. Необходимо также контролировать наличие паролей в сетевых каталогах.

Стоит учесть, что отдел так как генерацией паролей занимается отдел ИТ, то пользователи отдела могут рассылать пароли пользователям совершенно свободно, но только внутри компании.

Стандартизированные форматы паролей (кириллица):

6 букв – 1 знак !?#\$%^/_& – 2-4 цифры – 4 буквы – 2-3 знака !?#\$%^/_&
(например, ПаРоль#67pКнЕ!?)

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 11

Политика 12

Необходимо контролировать передачу определенных типов файлов только за пределы компании.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 12

Описание модуля F: Предотвращение инцидентов и управление событиями информационной безопасности

Задание 1: Контроль доступа

Необходимо создать пользователя DLP системы с определенными правами просмотра и редактирования.

Задание 2: Сводки

Создайте новые вкладки сводки в разделе «Сводка»

Задание 3: Виджеты

Создайте в сводке 4 виджета:

9. Выборка по событиям за период
10. Выборка по политикам с технологиями за период
11. Статистика за период
12. По нарушителям за период

Задание 4

Необходимо создать виджет отображающий события определенного типа (с определенного устройства и т. п.) за период.

Зафиксировать скриншотом конструктора выборки.

Задание 5

Необходимо создать виджет отображающий события определенного уровня (определенных политик и т. п.) за период.

С помощью технологии виртуальных машин для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах (Главный офис — виртуальные машины, Офис филиал — виртуальные машины).

При выполнении заданий необходимо ключевые настройки подтверждать скриншотами. Скриншоты необходимо сохранить на рабочем столе в папке «Модуль (номер)». Формат названия скриншотов: ITCS-1-2-1.jpg (задание 1.2, скриншот 1). Можно добавить комментарий (ITCS-1-2-1-Coordinator).

В ходе выполнения данного задания нужно установить основное ПО на рабочие станции будущей защищенной сети.

Доступ на все машины указан в дополнительной карточке задания

В случае изменения каких-либо логинов или паролей необходимо отобразить это в отчете.

Настройки сетевого окружения

Для правильной работы сети надо создать или убедиться в наличии 4 сетей:

- Host only или внутренняя сеть адаптер для сети центрального офиса
- Host only или внутренняя сеть адаптер для сети филиала
- Host only или внутренняя сеть адаптер для сети межсетевого взаимодействия
- Host only адаптер, NAT или Bridge для виртуального «Интернета» (в соответствии с инфраструктурой площадки, для связи всех координаторов между собой)

В случае иных настроек инфраструктуры экзаменационной площадки необходимо изменить данные сведения в задании!

IP адреса защищенных сетей

- Центральный офис «Сеть 1 ЦО»: 1.2.3.0/28
- Офис филиал «Сеть 1 Филиал»: 2.3.4.0/27
- Офис сеть 2 «Сеть 2 Офис»: 5.6.7.0/26
- «Интернет» для всех координаторов: 8.9.10.0/24

Адреса выбираются самостоятельно из указанного диапазона.

Необходимо записать все IP адреса, логины и пароли в текстовый файл VPN.txt на рабочем столе компьютера.

В связи с особенностями работы системы на серверных версиях необходимо устанавливать компоненты системы вручную (например, БД, сервер ЦУС, клиент ЦУС) используя пакеты MSI в подпапках дистрибутивов.

Описание модуля А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Задание 1.1. Развертывание ПК Administrator в качестве центра сертификации

Установить базу данных на VM Net1-DB (незащищенный узел)

Установить и настроить рабочее место администратора Certification Authority (на базе виртуальной машины Net1-Admin (ЦО)): Центр управления сетью

(серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД.

Установить клиент ЦУС на VM Net1-DB (незащищенный узел)

Если были произведены изменения паролей, IP-адресов и так далее, необходимо отразить это в отчете.

Задание 1.2. Установка ПО VPN Coordinator и ПО VPN Client для Certification Authority

1. установить ПО Client, рабочее место администратора;
2. установить и инициализировать ПО Coordinator HW-VA, допускается использование аппаратного координатора HW;

Задание 1.3. Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины

1. установить ПО Client.
2. установить ПО Publication Service.
3. установить ПО Registration Point.
4. установить ПО CA Informing.

Задание 1.4. Установка ПО Coordinator и ПО Client для организации сети филиала

1. установить и инициализировать ПО Coordinator HW-VA.
2. установить ПО Client, рабочее место пользователя.

Необходимо зафиксировать процесс установки скриншотами форм + сделать скриншот директории, в которую установлено ПО, и скриншот первого запуска приложения.

Задание 1.5. Развертывание удостоверяющего центра в составе сети

Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

Схема сети, которую требуется создать, приведена далее.

IP адреса сетей перечислены в начале задания (по названию сетей).

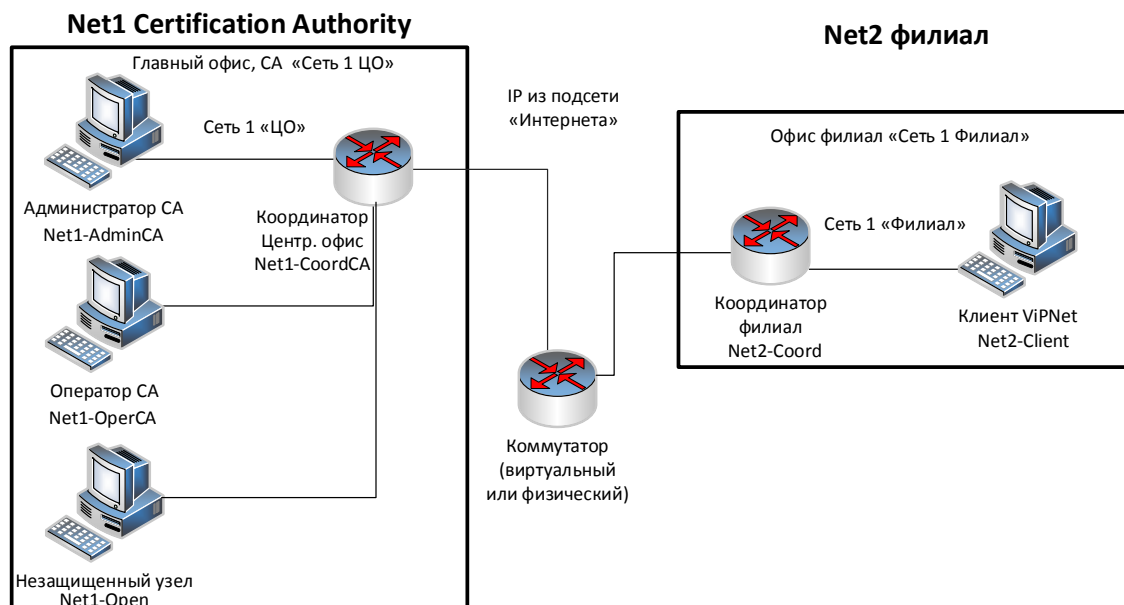


Рисунок 2 Схема защищенной сети

В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).

Таблица 2 Узлы защищенной сети если УКЦ и ЦУС на одной машине.

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1-AdminCA (ЦО)	Главный администратор (VM)	Administrator (ЦУС клиент и сервер + УКЦ), Client, CA Informing	ОС пользовательская или серверная	AdminCA
Net1-CoordCA (ЦО)	Координатор Центр Офис (VM)	Coordinator	Координатор HW-VA	CoordinatorCA
Net1-OperCA (ЦО)	Оператор УЦ (VM)	Client, Publication Service, Registration Point	ОС пользовательская или серверная	OperCA
Net2-Coord (Филиал)	Координатор Филиал (VM)	Coordinator	Координатор HW-VA	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал (VM)	Client	ОС пользовательская или серверная	User

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	Coordinator Office	Admin	OperCA	Coordinator Subsidiary	User
CoordinatorOffice	×	*	*	*	
Admin	*	×	*		*
OperCA	*	*	×	*	
CoordinatorSub	*		*	×	*
User		*		*	×

Задание 1.6. Создание структуры защищенной сети

ЦУС. Необходимо создать в ЦУС структуру защищенной сети в соответствии с заданной схемой (выгрузить отчет в HTML). Создать пользователей узлов, настроить полномочия пользователей и их связи в соответствии со схемой.

УКЦ. Провести инициализацию УКЦ, сохранить контейнер ключей администратора в общей папке (создать подпапку Задание 1.6), поменять тип паролей для пользователей («собственный»). Задать пароли пользователей и сохранить в текстовый файл. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить на жесткий диск). Создать группы узлов для центрального офиса (удостоверяющего центра) и филиала, настроить пароль администратора группы сетевых узлов для каждой из групп (проверить, что пароль работает).

На всех узлах сети корректно настроить или проверить корректность настройки сетевых интерфейсов в соответствии со схемой, проверить доступность соседних узлов.

Разнести DST файлы по АРМ, провести первичную инициализацию узлов защищенной сети (координаторов и клиентов), проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов.

Задание 1.7. Настройка работы удостоверяющего центра в аккредитованном режиме

Необходимо перевести УКЦ в режим аккредитованного удостоверяющего центра, настроить параметры издания квалифицированных сертификатов, указав:

- сведения о средствах УЦ,
- средство электронной подписи издателя
- средства удостоверяющего центра
- сертификат на средство электронной подписи издателя
- сертификат на средство удостоверяющего центра
- класс защищенности, которому соответствуют программные средства УЦ,
- место хранения контейнеров ключа ЭП и ключа защиты УКЦ

После перевода УКЦ в аккредитованный режим необходимо выпустить:

- Корневой квалифицированный сертификат.
- Квалифицированную электронную подпись для пользователя
- Квалифицированную электронную подпись для пользователя

При формировании сертификатов необходимо заполнить следующие поля:

- Имя: <Имя пользователя или узла>
- Электронная почта
- Город
- Область
- Организация
- Подразделение
- Почтовый индекс

Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети. Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации (Publication Service).

Реализовать автоматическую публикацию сертификатов.

Посредством Центра Регистрации (Registration Point):

6. зарегистрировать пользователя;
7. отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос;
8. отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос.

Посредством Сервиса Информирования (CA Informing):

9. настроить способ выдачи уведомлений;
10. сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов

Задание 1.8. Модификация структуры защищенной сети

Перед началом выполнения сделать HTML выгрузку структуры сети и сделать скриншот ЦУС окна с пользователями.

Модификация структуры сети:

5. добавить новый сетевой узел и пользователя за координатором (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем. На указанных узлах проверить появление нового узла;
6. Добавить пользователя на узле Филиал (Net2-Client филиала 2), связать его со всеми пользователями группы узлов центральный офис. Для указанных пользователей проверить появление новой связи;
7. отправить письмо по Деловой почте пользователю.
8. отправить текстовое сообщение пользователю

Необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:

- скриншоты деловой почты на отправителе и получателе (при отправке письма);
- скриншоты текстового сообщения на отправителе и получателе;
- скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы.

Кроме того, необходимо сохранить файл HTML с обновленной структурой защищенной сети, выгруженный из ЦУС.

Описание модуля D: Технологии защиты и анализа сетевого трафика

Задание 2.1. Компрометация узла защищенной сети

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя, т. к. в случае неудачной компрометации структура сети может нарушиться.

Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС:

5. скомпрометировать ключи пользователя на узле,
6. произвести смену ключей пользователя и сетевых узлов,
7. отправить обновления и произвести процедуру смены ключа пользователя,
8. проверить работу защищенной сети после обновления отправив сообщение от пользователя.

Восстановление взаимодействия с помощью ручной установки DST засчитано не будет.

Необходимо зафиксировать процесс настройки скриншотами или иным указанным способом:

- компрометация пользователя.
- смена ключей пользователя и сетевых узлов.
- процедура смены ключа на клиенте с использованием резервного набора ключей.
- скриншот экрана «защищенная сеть» в Monitor на узле Пользователь_2 Филиал + результат проверки доступности узлов.

Кроме того, нужно сохранить архив директории, в которой расположен резервный набор ключей на рабочем столе компьютера (после смены ключей).

Задание 2.2. Межсетевое взаимодействие защищённых сетей (со связями «все со всеми»)

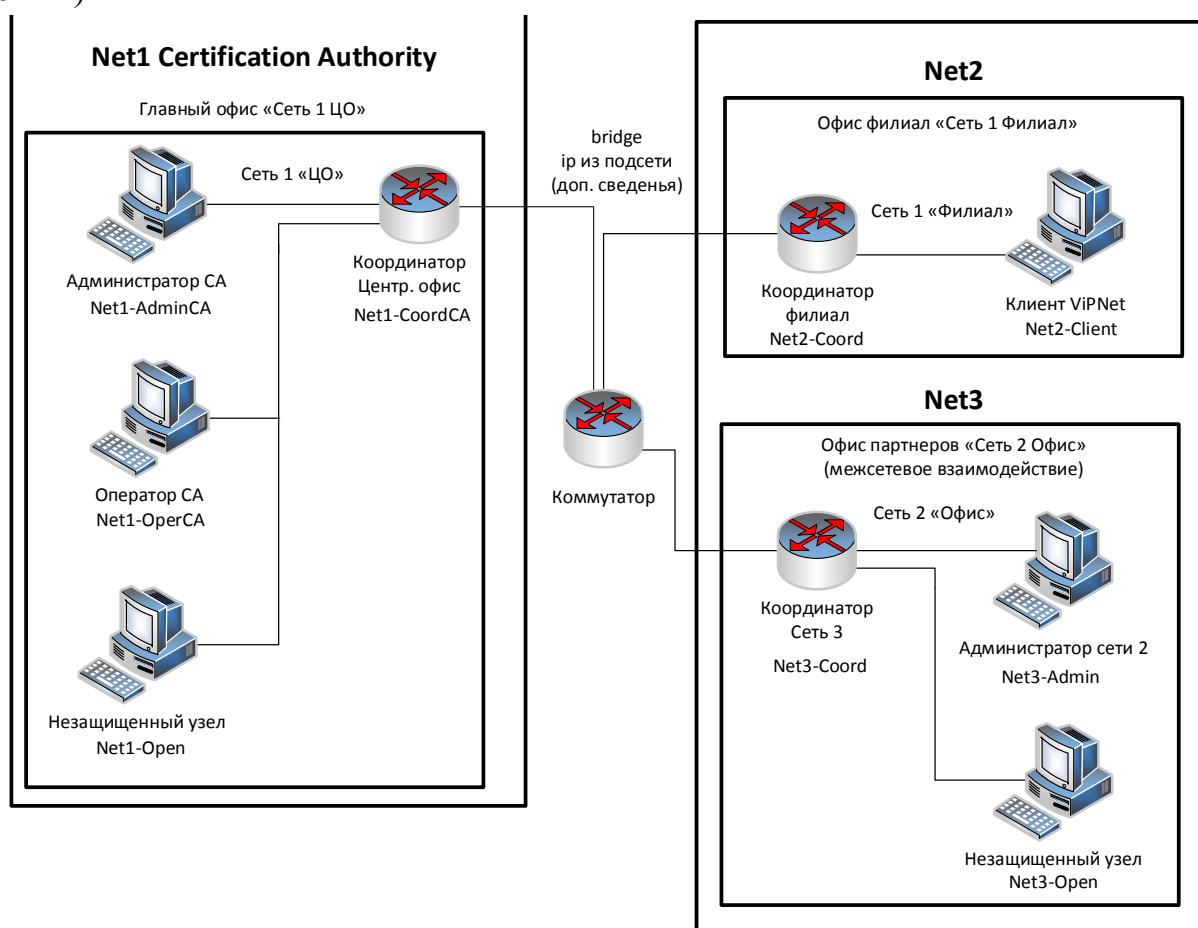


Рисунок 2 Схема межсетевого взаимодействия

Развернуть на Net3-Admin (Сеть 3 межсеть) на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети:

Рабочее место администратора (БД, ЦУС, УКЦ, Client)

- 1 координатор (HW-VA),
- 1 узел Admin,
- Установите координатор.

Установить и настроить необходимое ПО

Настроить межсетевое взаимодействие между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.

Проверить взаимодействие узлов, отправив сообщение деловой почты.

Задание 2.3. Туннелирование в рамках межсетевого взаимодействия

Подключить незащищенную машину в сети 3.

Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по зашифрованному каналу.

Проверить доступность незащищённых машин друг другу любым другим протоколом; проанализировать журналы IP-пакетов на координаторах.

Скриншоты:

- Настройка максимального количества туннелей на координаторах
- Скриншоты прохождения ICMP пакетов (ping) и любого другого трафика с незащищенного узла
- Скриншоты журнала IP-пакетов координатора с установленным фильтром «Туннелирование» для проверки прохождения ICMP-пакетов и любого другого трафика с помощью туннелирования

Необходимые приложения

Приложение 1: Карточка настроек сети и оборудования (docx)

Приложение 2: Шаблоны документов для задания (zip)