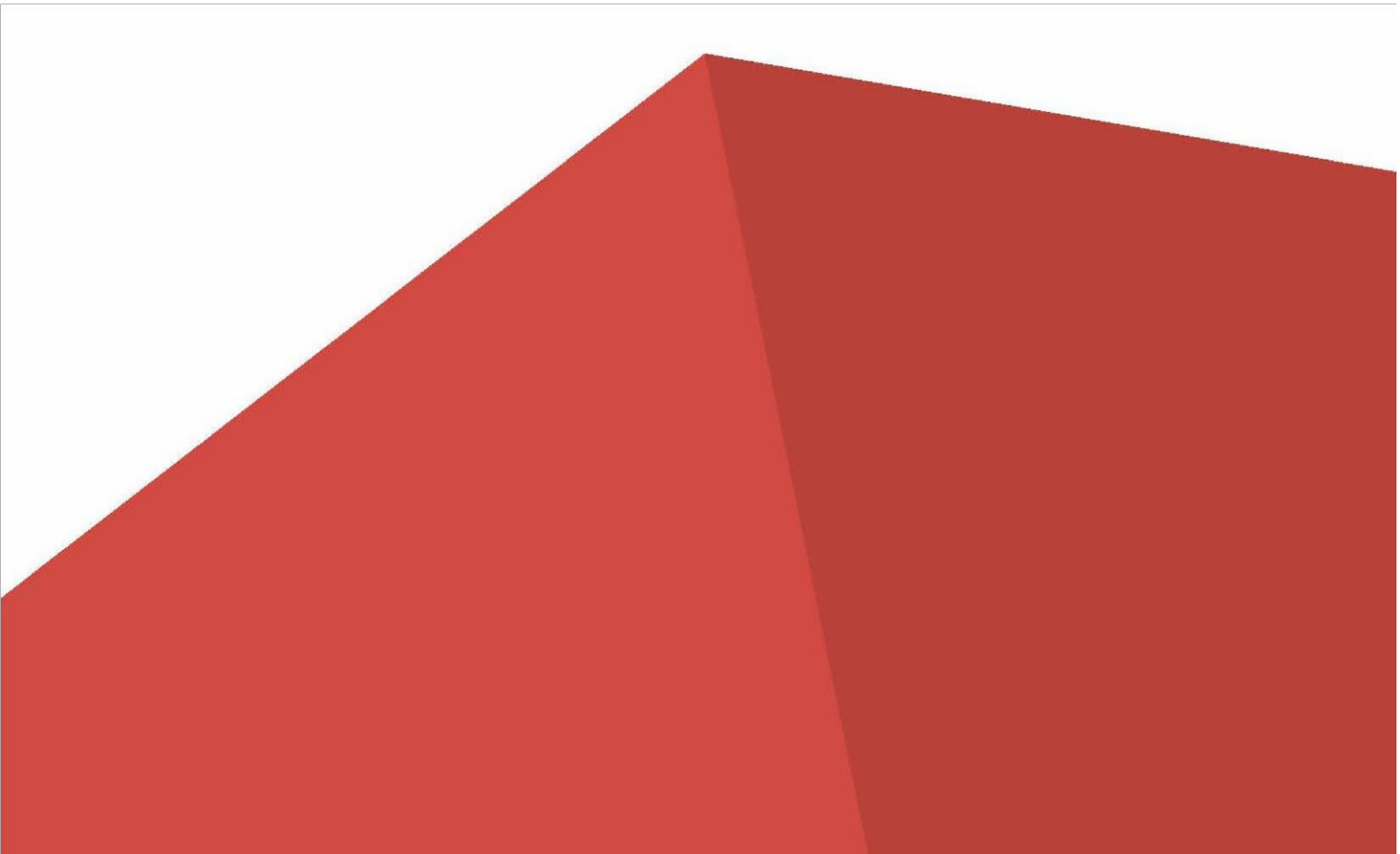
УТВЕРЖДЕНО

Решением Рабочей группы по вопросам разработки оценочных материалов для проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия по образовательным программам среднего профессионального образования
(Протокол от 24.12.2020 г.
№ Пр-24.12.2020-1)

Оценочные материалы для Демонстрационного Экзамена по стандартам Ворлдскиллс Россия по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»



Инструкция по охране труда и технике безопасности для проведения Демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Содержание

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 уведомляется Главный эксперт. 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 завершенную 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 

- EC 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 участником норм и правил ОТ и ТБ ведет к потере баллов. Постоянное нарушение норм безопасности может привести к временному или перманентному отстранению аналогично апелляции.

2. Требования охраны труда перед началом выполнения работ

Перед началом выполнения задания участники должны выполнить следующее:

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 удается, 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 действующие 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:

- надеть 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 удается, 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.

Комплект оценочной документации № 1.1 для Демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

СОДЕРЖАНИЕ

Паспорт комплекта оценочной документации (КОД) № 1.1 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Комплект оценочной документации (КОД) № 1.1 разработан в целях организации и проведения демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» и рассчитан на выполнение заданий продолжительностью 6,5 часов.

КОД № 1.1 может быть рекомендован для оценки освоения основных профессиональных образовательных программ и их частей, дополнительных профессиональных программ и программ профессионального обучения, а также на соответствие уровням квалификации согласно Таблице (Приложение).

1. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации № 1.1 (Таблица 1).

Таблица 1.

Раздел WSSS	Наименование раздела WSSS	Важность (%)
1	**Организация работы и управление**	**3**
2	**Установка, конфигурирование и устранение неисправностей**	**15**
4	**Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**	**20,8**
6	**Технологии агентского мониторинга**	**13**
7	**Анализ выявленных инцидентов. Подготовка отчетов, классификация угроз и инцидентов**	**2,2**

Таблица 2.

Раздел WSSS	Наименование раздела WSSS
1.	Организация работы и управление
	Специалист должен знать и понимать: • Понимание принципов работы специалиста по информационной безопасности и их применение; • Знание принципов и положений безопасной работы в общем и по отношению к корпоративной среде;

	• Регламентирующие документы в области безопасности информационных систем; • Регламентирующие документы в области охраны труда и безопасности жизнедеятельности; • Важность организации труда в соответствии с методиками; • Методы и технологии исследования; • Важность управления собственным профессиональным развитием; • Скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню. • Важность умения слушать собеседника как части эффективной коммуникации; • Роли и требования коллег, и наиболее эффективные методы коммуникации; • Важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими; • Способы разрешения непонимания и конфликтующих требований; • Методы управления стрессом и гневом для разрешения сложных ситуаций.
	Специалист должен уметь: • Поддерживать безопасную, аккуратную и эффективную рабочую зону; • Использовать все оборудование и программное обеспечение безопасно и в соответствии с инструкциями производителя; • Следовать предписаниям в области охраны труда и безопасности жизнедеятельности; • Регулярно планировать свою работу и корректировать планы в соответствии с изменяющимися приоритетами; • Поддерживать рабочее место в должном состоянии и порядке. • Демонстрировать развитые способности слушать и задавать вопросы для более глубокого понимания сложных ситуаций; • Выстраивать эффективное письменное и устное общение; • Понимать изменяющиеся требования и адаптироваться к ним;
2.	Установка, конфигурирование и устранение неисправностей
	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 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 Windows Server и Linux Red Hat Enterprise Linux; • 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;
4.	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз
	Специалист должен знать и понимать: • Технологии работы с политиками информационной безопасности; • Создание новых политик, модификация существующих; • Общие принципы при работе интерфейсом системы защиты корпоративной информации; • Объекты защиты, персоны; • Ключевые технологии анализа трафика; • Типовые протоколы и потоки данных в корпоративной среде, такими как: • корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4) • веб-почта; • Интернет-ресурсы: сайты, блоги, форумы и т. д. (протоколы HTTP, HTTPS); • социальные сети; • интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP; • принтеры: печать файлов на локальных и сетевых принтерах; • любые съемные носители и устройства; • Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек; • Типы угроз информационной безопасности, типы инцидентов, • Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации; • Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации; • Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных; • Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации; • Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки; • Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе; • Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов; • Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации;
	Специалист должен уметь: • Создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты; • Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; • Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; • Работа со сводками, виджетами, сводками; • Работа с персонами;

	• Работа с объектами защиты; • Провести имитацию процесса утечки конфиденциальной информации в системе; • Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; • Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. • Работа с категориями и терминами; • Использование регулярных выражений; • Использование морфологического поиска; • Работа с графическими объектами; • Работа с выгрузками и баз данных; • Работа с печатями и бланками; • Работа с файловыми типами; • Эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;
6.	Технологии агентского мониторинга
	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.
	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.
7.	Анализ выявленных инцидентов. Подготовка отчетов, классификация угроз и инцидентов
	Специалист должен знать и понимать: • Основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах; • Инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз; • Типовой пакет нормативных документов, необходимого для развёртывания и эксплуатации системы корпоративной защиты в организации; • Виды типовых отчетных форм о выявленных угрозах и инцидентах; • Типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации; • Понимать подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз;

	• Системы DLP и требования по информационной безопасности. • Категорирование информации в РФ. • Юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; Специальные технические средства • Меры по обеспечению юридической значимости DLP (Pre-DLP). • Практику право применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (Post-DLP).
	Специалист должен уметь: • Разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности; • Проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации; • Создавать отчёты о выявленных инцидентах, угрозах и т.п. • Представлять отчёты руководству, обосновывать полученные результаты анализа.

2. Формат Демонстрационного экзамена:

Очный

3. Форма участия:

Индивидуальная

4. Вид аттестации:

ГИА

5. Обобщенная оценочная ведомость.

В данном разделе определяются критерии оценки и количество начисляемых баллов (судейские и объективные) (Таблица 3).

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 54.

Таблица 3.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
1.	1. Установка и конфигурирование компонентов DLP системы	A. Организация работы и управление B. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	2 часа	1, 2	0	18	18
2.	2. Технологии агентского мониторинга	C. Технологии агентского мониторинга	1,5 часа	6	0	13	13
3.	3. Разработка и применение политик, анализ выявленных инцидентов	D. Разработка политик безопасности, анализ выявленных инцидентов	3 часа	4, 7	0	23	23
				Итого		54	54

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

6.1. Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» — 3 чел.

6.2. Расчет количества экспертов исходя из количества рабочих мест и участников осуществляется по схеме согласно Таблице 4:

Таблица 4.

Количество постов-рабочих мест / Количество участников	1-5	6-10	11-15	16-20	21-25
От 1 до 5	3				
От 6 до 10		3			
От 11 до 15			4		
От 16 до 20				5	
От 21 до 25					6

7. Список оборудования и материалов, запрещенных на площадке

- Мобильные телефоны, смартфоны, рации, беспроводные, проводные наушники и другие средства связи;
- Собственные заметки, шпаргалки, книги и прочие документы;
- Личная электронная почта, мессенджеры и прочие средства связи посредством сети Интернет за исключение разрешенных ресурсов для тестирования систем в процессе работы;
- Компьютеры, ноутбуки, планшеты и прочие устройства, за исключением устройств, предоставленных площадкой;
- Периферийные устройства (клавиатуры, манипуляторы типа мышь и прочие устройства) за исключением устройств, предоставленных площадкой.

Задание для демонстрационного экзамена по комплекту оценочной документации № 1.1 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

(образец)

Задание включает в себя следующие разделы:

1. Формат Демонстрационного экзамена
2. Формы участия
3. Вид аттестации
4. Модули задания, критерии оценки и необходимое время
5. Необходимые приложения

Продолжительность выполнения задания: 6,5 ч.

8. Формат Демонстрационного экзамена:

Очный

9. Форма участия:

Индивидуальная

10. Вид аттестации:

ГИА

11. Модули задания, критерии оценки и необходимое время

Модули и время сведены в Таблице 1.

Таблица 1.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
1.	1. Установка и конфигурирование компонентов DLP системы	A. Организация работы и управление B. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	2 часа	1, 2	0	18	18
2.	2. Технологии агентского мониторинга	C. Технологии агентского мониторинга	1,5 часа	6	0	13	13
3.	3. Разработка и применение политик, анализ выявленных инцидентов	D. Разработка политик безопасности, анализ выявленных инцидентов	3 часа	4, 7	0	23	23
				Итого		54	54

Модули с описанием работ

Модуль 1: Установка и конфигурирование компонентов DLP системы

Введение

В компания «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 носители информации, электронная почта и различные интернет-ресурсы.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены, но IP адреса нужно назначить согласно прилагаемой карточке. Подготовлены следующие виртуальные машины для дальнейшей работы:

AD Сервер с контроллером домена

DLP сервер установлен (но не настроен), активирована лицензия

Виртуальная машина для установки сервера агентского мониторинга

Виртуальные машины «нарушителей» для установки агентов

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов. До установки системы необходимо подготовить доменных пользователей в соответствии с заданием.

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 номером рабочего места (например, server-16).

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

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например: Задание_5_копирование.jpg.

Задание 1: Настройка контроллера домена

Необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: user1, пароль: 12345678, запретить локальный вход в систему

Логин: user2, пароль: 12345678, запретить локальный вход в систему

Логин: user3, пароль: 12345678, права администратора домена и локального администратора

Логин: user4, пароль 12345678, права пользователя домена

Задание 2: Настройка DLP сервера

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

Необходимо вычислить IP-адрес сервера через локальную консоль виртуальной машины.

Настроить DNS на сервере для корректной работы.

Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам.

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

Для входа в веб-консоль необходимо использовать ранее созданного пользователя домена с полными правами 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» с заголовком IWTM.

Корректно выполненным заданием будет являться работоспособная система с верно настроенными параметрами.

Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить базу данных с паролем суперпользователя 12345678.

Установить сервер агентского мониторинга с параметрами по умолчанию.

При установке необходимо установить соединение с DLP-сервером контроля сетевого трафика по IP-адресу и токену, но можно сделать это и после установки сервера агентского мониторинга.

Настроить пользователя консоли управления: officer с паролем 12345678.

Синхронизировать каталог пользователей и компьютеров с Active Directory.

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

Зафиксировать факт создания пользователя и настройку скриншотом.

Проверить работоспособность входа в консоль управления без ввода пароля. Стоит обратить внимание, что если сервер не введен в домен, данная опция работать не будет.

Зафиксировать факт подключения без пароля скриншотом.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» с заголовком IWDM.

Задание 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить агент мониторинга с помощью задачи первичного распространения с сервера агентского мониторинга. Необходимо учесть, что установка осуществляется только с правами администратора (доменного или локального). Ручная установка с помощью создания пакета установки является неверным выполнением задания.

Зафиксировать успешное выполнение задачи скриншотом

В случае проблем стоит проверить настройки брандмауэра и DNS.

Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)

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

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

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога.

Зафиксировать выполнение задания скриншотом настройки в web-консоли.

Стоит учесть, что неправильная настройка DNS на серверных машинах, а также неправильные настройки брандмауэра могут привести к неработоспособной системе сканирования сетевых ресурсов.

Задание 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания событий) для данных, содержащих слово «Экзамен», установить низкий уровень угрозы для всех событий, добавить тег «Экзамен».

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

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена).

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задание 7: Защита системы с помощью сертификатов

Создайте цифровой сертификат (дерево сертификатов) формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности, длине ключа 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)
- сертификат сервиса (веб-сайта)

Итоговый результат должен включать:

- Дерево из 2 (3)-х сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов.

- Содержимое команд по генерации ключей и сертификатов в текстовом файле «отчет.txt»
- Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе просмотра сертификатов Windows (закладки «Общие», «Путь сертифкации»).

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

Генерацию сертификатов зафиксируйте скриншотами.

Модуль 2: Технологии агентского мониторинга

Задания выполняются только с помощью компонентов DLP системы (не групповыми политиками или аналогичными решениями).

Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т.д. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т.д.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 2».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CP-1.jpg

где CP – сокращение от англ. creating a policy, 1 – номер задания

Пример 2 для сохранения скриншота работающей политики: PW-1.jpg

где PW – сокращение от англ. policy work, 1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики:

PW-1-2.jpg

где PW – сокращение от англ. policy work, 1 – номер задания; 2 – номер скриншота для задания 1.

Задание 1

Необходимо создать новую политику, применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику.

Зафиксировать выполнение скриншотом.

Задание 2

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

Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли с указанием адреса.

Задание 3

Для удаленного управления необходимо создать дополнительного локального офицера безопасности для доступа к серверу агентского мониторинга с полными правами на управление и просмотр разделов.

Имя пользователя: user1, пароль: 12345678

Проверить работоспособность с удаленной консоли, установленной ранее, зафиксировать выполнение скриншотом.

Задание 4

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 5

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 6

Необходимо поставить на контроль буфер обмена в текстовых процессорах.

Проверить работоспособность и зафиксировать выполнение занесением пары событий в веб-консоль DLP-сервера на любые политики. Также подтвердить выполнение скриншотом.

Задание 7

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Задание 8

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 9

С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе.

Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.

Задание 10

Создать политику по блокировке копирования файлов формата zip на USB-накопители.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 11

Необходимо поставить на контроль печать документов на принтерах. Продемонстрировать работоспособность на любую из политик.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 12

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 15 секунд или при переходе на другую страницу.

Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в веб-консоли DLP-сервера. Подтвердить выполнение задания скриншотами.

Задание 13

Заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 14

Осуществить выдачу временного доступа (30 минут) клиенту до заблокированного CD привода.

Зафиксировать скриншотами факт выдачи доступа и необходимые действия для выдачи доступа.

Задание 15

На машине нарушителя необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 16

Необходимо установить (сменить) пароль для удаления агента мониторинга на машине нарушителя с помощью средств сервера агентского мониторинга (удаленно).

Проверить работоспособность и зафиксировать выполнение скриншотом

Модуль 3: Разработка и применение политик, анализ выявленных инцидентов

Введение

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Для некоторых политик необходима работа с разными разделами консоли управления: категориями и терминами, технологиями, объектами защиты и т. п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, необходимо самостоятельно задать уровень угрозы).

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации с AD-сервером компании

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, т. к. легальные события не должны маркироваться как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Проверьте синхронизацию времени на всех системах, т. к. расхождение во времени между системами может повлиять на актуальность событий.

Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти в папке «Additional files» в общей папке из дополнительных сведений.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 3».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: 01-CP.jpg

где CP – сокращение от англ. creating a policy, 01 – номер задания

Пример 2 для сохранения скриншота работающей политики: 04-PW-1.jpg, 04-PW-2.jpg, где PW – сокращение от англ. policy work, 04 – номер задания, 1,2 – номер скриншотов

Задания на разработку политик можно выполнять в любом порядке.

ВНИМАНИЕ!

Необходимо называть политики / объекты / категории / теги и прочее ТОЛЬКО в соответствии с номером и названием задания

Политики — Политика X, например «Политика 4».

Для комбинированных политик формат: Политика 4.1, 4.2 и т.д.

Объект защиты — Объект X, например «Объект 11».

ВНИМАНИЕ!

Все политики «по умолчанию», находящиеся в консоли управления в процессе выполнения заданий должны быть отключены или удалены, так как могут помешать корректной оценке.

ВНИМАНИЕ!

При разработке и тестировании политик стоит учитывать, что нарушителем могут являться не только указанные в задании пользователи, а еще и виртуальная машина с агентом мониторинга.

ВНИМАНИЕ!

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.

Задание 1

Создайте локальную группу пользователей «Сотрудники под наблюдением». Добавьте в нее трех любых пользователей. Подтвердите выполнение задания скриншотами.

Задание 2

Для работы системы необходимо настроить периметр компании:

Почтовый домен: demo.lab.

Список веб ресурсов необходимо создать и назвать «Доверенные домены»: worldskills.org, filialdemo.lab, demolab-info.ru, dlpsystems.lab.

Группа персон 1: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Задание 3

Для недавно нанятого аудитора компании необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей без возможности редактирования. Области видимости: все.

Логин: auditor, пароль: 12345678

Подтвердите выполнение задания скриншотами.

Политика 4

В связи с секретностью при организации очередного WorldSkills, совет директоров решил контролировать передачу информации о WorldSkills за пределы компании. В связи с этим необходимо создать политику на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills».

Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять пробел между словами, например: «Ворлд Skills». Ложных срабатываний быть не должно (например, просто на Ворлд или Skills).

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: мобильники

Проверить работоспособность.

Политика 5

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%.

Для пустого документа:

Вердикт: разрешить √

Уровень нарушения: нет

Тег: договор

Для заполненного документа:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: договор

Проверить работоспособность.

Политика 6

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании, запрещая любую внешнюю передачу документов, содержащих заполненные бланках, при этом пустые бланки контролировать не нужно.

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 7

Для мониторинга движения официальных документов необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Политика 8

В компании происходит передача сообщений, содержащих специальные коды доступа к внутренней информационной системе. Все коды находятся в документе «Коды компании» (10 штук). Необходимо контролировать коды внутри компании, но запрещать передачу за пределы.

Передача кодов внутри компании:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: коды

Передача кодов за пределы компании:

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 9

Ракетное вооружение для авиационных комплексов различного класса, в разработке которого участвует компания, планируется к внедрению в эксплуатацию. Информация о технике может иметь конфиденциальный и секретный характер, хотя и не содержать гриф.

Необходимо блокировать любые попытки передачи данных об этих объектах на внешние адреса. Технические объекты задаются буквенно-цифирными кодами на русском языке:

Р-Цифры-Буквы или РЦифрыБуква или Р-ЦифрыБуква

- Р – русская буква «Р»
- Цифры – не более 4-х подряд, например, 27 или 5000 (обязательно наличие хотя бы одной цифры)
- Буквы – от 1 до 2-х подряд, например, Р-27АЭ

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: ракеты

Проверить работоспособность.

Политика 10

Сотрудники отдела ИТ 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 отдела информатизации.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: база

Проверить работоспособность.

Политика 11

В связи с постоянными заказами на транспортировку больших грузов, сотрудники компании подрабатывают в тайне от начальства, занимаясь попутной перевозкой других грузов, а также пассажиров. В связи с этим необходимо отслеживать в почтовых сообщениях упоминания об автостопе, халтуре, подработке, грузовом такси.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: подработка

Проверить работоспособность.

Политика 12

Необходимо запретить передачу документов с грифом (информационной меткой) «ООО Demo Lab. Конфиденциально» или «ООО Demo Lab. Строго конфиденциально» любым сотрудникам за пределы компании. Обратите внимание, что при вводе информационной метки с клавиатуры сотрудники могут ошибаться и вводить между словами более 1 пробела или табуляции, а также писать название компании на русском языке, например, «ООО Demo Лаб», «ООО Демо Лаб».

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: печать

Проверить работоспособность.

Политика 13

В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу. Необходимо отслеживать следующие термины: COVID, COVID-19, коронавирус, коронавирусная инфекция.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: вирус

Проверить работоспособность.

Политика 14

Для защиты персональных данных сотрудников необходимо запрещать всем, кроме отдела кадров передавать информацию, содержащую данные паспортов (в том числе и сканы/фото), а также СНИЛС и ИНН.

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: пдн

Проверить работоспособность.

Политика 15

Необходимо контролировать передачу документов формата электронных таблиц (исключая csv файлы!), а также CAD-документации. Стоит учесть, что файлы могут передаваться в том числе и на съемных носителях информации.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Задание 16: Анализ инцидентов, обычные сводки

Создайте новую вкладку сводки в разделе «Сводка» под названием «Экзамен» и создайте в ней 4 виджета:

Динамика активности по событиям за последнюю неделю

Статистика по политикам за последние 7 дней

По типу событий: необработанные нарушения за три дня

По топ-нарушителям за текущий месяц.

Задание 17: Анализ инцидентов, специальные выборки

Необходимо создать новую вкладку в разделе «Сводка» под названием «Особые выборки» и добавить в нее виджеты:

Отображающий события с уровнем угрозы от низкого до высокого на правила копирования (внешние носители, печать) за последние 7 дней.

Отображающий события с любым одним тегом.

5. Необходимые приложения

Приложение 1 Пояснения по подготовке площадки (документ docx)

Приложение 2 Карточка настроек сети и оборудования (документ docx)

Приложение 3 Эталонные файлы для выполнения заданий (архив zip)

Приложение 4 Пример пользователей и групп для домена (документ csv)

Примерный план работы[1] Центра проведения демонстрационного экзамена по КОД № 1.1 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

	Примерное время	Мероприятие
Подготови-тельный день	08:00	Получение главным экспертом задания демонстрационного экзамена
	08:00 – 09:00	Проверка готовности проведения демонстрационного экзамена, заполнение Акта о готовности площадки
	09:00 – 09:15	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение протоколов
	09:15 – 09:30	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах
	09:30 – 09:45	Регистрация участников демонстрационного экзамена
	09:45 – 10:15	Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	10:15 – 12:00	Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение протоколов
	12:00 – 16:00	Подготовка и/или проверка работоспособности площадки в соответствии с заданием
День 1	08:45 – 09:00	Ознакомление с заданием и правилами
	09:00 – 09:15	Брифинг
	09:15 – 11:15	Выполнение модуля 1
	11:15 – 11:30	Перерыв, обработка помещения, проветривание
	11:30 – 13:00	Выполнение модуля 2
	13:00 – 13:45	Обед, обработка помещения, проветривание
	13:45 – 15:30	Выполнение модуля 3
	15:30 – 15:45	Перерыв, обработка помещения, проветривание
	15:45 – 17:00	Выполнение модуля 3
	17:00 – 19:00	Работа экспертов, заполнение форм и оценочных ведомостей
	19:00 – 20:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола Подготовка площадки для следующей экзаменационной группы (при наличии)

[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.

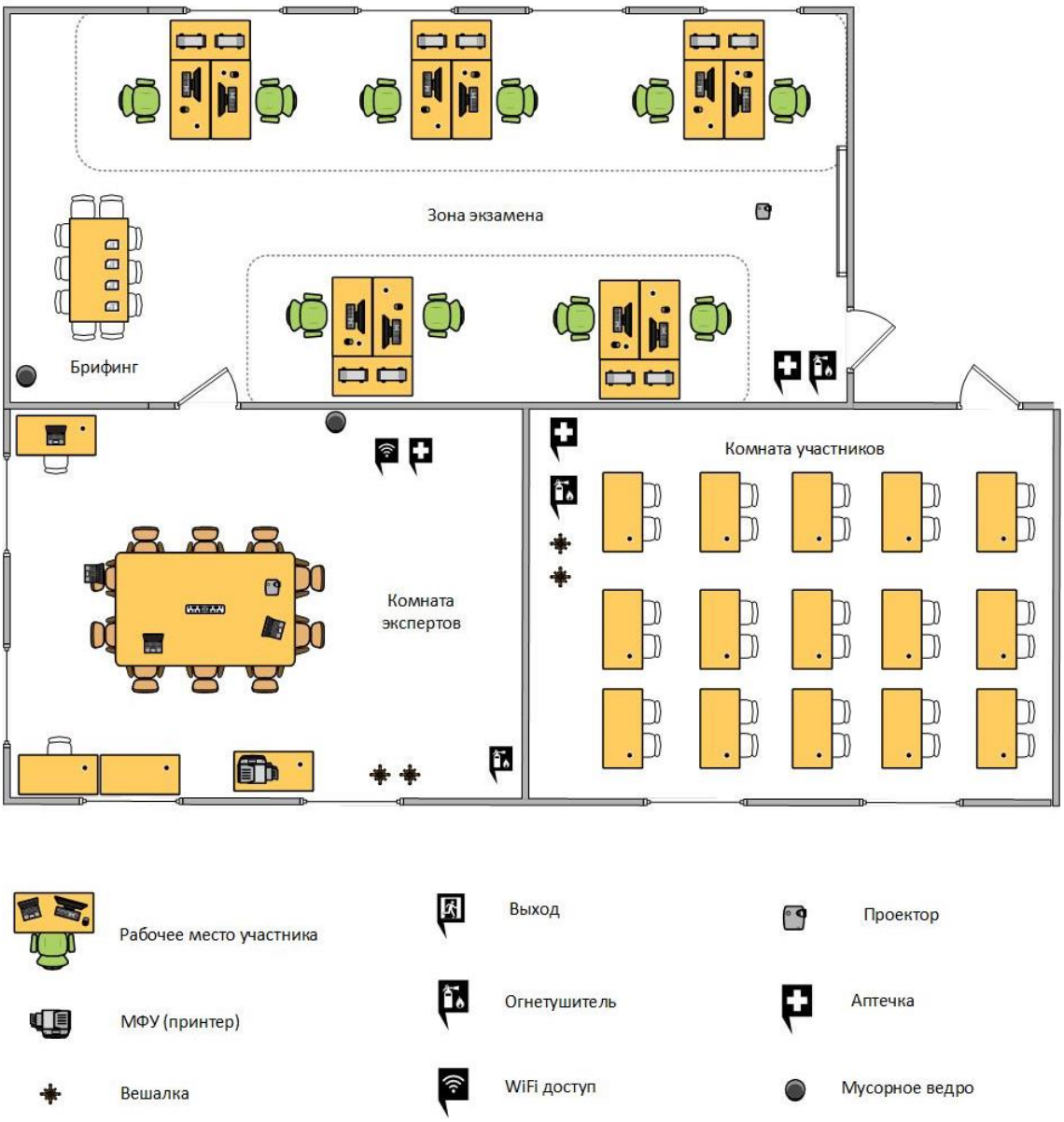
План застройки площадки для проведения демонстрационного экзамена по КОД № 1.1 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Номер компетенции: F7

Название компетенции: Корпоративная защита от внутренних угроз информационной безопасности

Общая площадь площадки: 100 м^2

План застройки площадки:



Приложения

Инфраструктурный лист для КОД № 1.1 (документ xlsx)

Пояснения по подготовке площадки для КОД № 1.1 (документ docx)

Карточка настроек сети и оборудования для КОД № 1.1 (документ docx)

Эталонные файлы для выполнения заданий для КОД № 1.1 (архив zip)

Пример пользователей и групп для домена (документ csv)

Комплект оценочной документации № 1.2 для Демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

СОДЕРЖАНИЕ

Паспорт комплекта оценочной документации (КОД) № 1.2 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Комплект оценочной документации (КОД) № 1.2 разработан в целях организации и проведения демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» и рассчитан на выполнение заданий продолжительностью 5,5 часов.

КОД № 1.2 может быть рекомендован для оценки освоения основных профессиональных образовательных программ и их частей, дополнительных профессиональных программ и программ профессионального обучения, а также на соответствие уровням квалификации согласно Таблице (Приложение).

1. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации № 1.2 (Таблица 1).

Таблица 1.

Раздел WSSS	Наименование раздела WSSS	Важность (%)
1	**Организация работы и управление**	**3**
2	**Установка, конфигурирование и устранение неисправностей**	**5,3**
5	**Технологии анализа и защиты сетевого трафика**	**19,7**

Таблица 2.

Раздел WSSS	Наименование раздела WSSS
1.	Организация работы и управление
	Специалист должен знать и понимать: • Понимание принципов работы специалиста по информационной безопасности и их применение; • Знание принципов и положений безопасной работы в общем и по отношению к корпоративной среде; • Регламентирующие документы в области безопасности информационных систем; • Регламентирующие документы в области охраны труда и безопасности жизнедеятельности;

	• Важность организации труда в соответствии с методиками; • Методы и технологии исследования; • Важность управления собственным профессиональным развитием; • Скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню. • Важность умения слушать собеседника как части эффективной коммуникации; • Роли и требования коллег, и наиболее эффективные методы коммуникации; • Важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими; • Способы разрешения непонимания и конфликтующих требований; • Методы управления стрессом и гневом для разрешения сложных ситуаций.
	Специалист должен уметь: • Поддерживать безопасную, аккуратную и эффективную рабочую зону; • Использовать все оборудование и программное обеспечение безопасно и в соответствии с инструкциями производителя; • Следовать предписаниям в области охраны труда и безопасности жизнедеятельности; • Регулярно планировать свою работу и корректировать планы в соответствии с изменяющимися приоритетами; • Поддерживать рабочее место в должном состоянии и порядке. • Демонстрировать развитые способности слушать и задавать вопросы для более глубокого понимания сложных ситуаций; • Выстраивать эффективное письменное и устное общение; • Понимать изменяющиеся требования и адаптироваться к ним;
2.	Установка, конфигурирование и устранение неисправностей
	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 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 Windows Server и Linux Red Hat Enterprise Linux; • 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;
5.	**Технологии анализа и защиты сетевого трафика**
	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 • Технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений; • Ключевые компоненты VPN-сетей; • Особенности VPN-сети и механизмы их управления; • Современные криптографические алгоритмы. Криптопровайдеры, криптографические интерфейсы и библиотеки; • Архитектура, основные компоненты PKI их функции и взаимодействие; • Жизненный цикл ключей и сертификатов; • Электронный сертификат ключей ЭЦП. 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; • 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;

2. Формат Демонстрационного экзамена:

Очный

3. Форма участия:

Индивидуальная

4. Вид аттестации:

ГИА

5. Обобщенная оценочная ведомость.

В данном разделе определяются критерии оценки и количество начисляемых баллов (судейские и объективные) (Таблица 3).

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 28.

Таблица 3.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
1.	1. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	A. Организация работы и управление B. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	2,5 часа	1. 2. 5.	0	15,3	15,3
2.	2. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	C. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	3 часа	2. 5.	0	12,7	12,7
				Итого		28	28

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

6.1. Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» — 3 чел.

6.2. Расчет количества экспертов исходя из количества рабочих мест и участников осуществляется по схеме согласно Таблице 4:

Таблица 4.

Количество постов-рабочих мест / Количество участников	1-5	6-10	11-15	16-20	21-25
От 1 до 5	3				
От 6 до 10		3			
От 11 до 15			4		
От 16 до 20				5	
От 21 до 25					6

7. Список оборудования и материалов, запрещенных на площадке

- Мобильные телефоны, смартфоны, рации, беспроводные, проводные наушники и другие средства связи;
- Собственные заметки, шпаргалки, книги и прочие документы;
- Личная электронная почта, мессенджеры и прочие средства связи посредством сети Интернет за исключение разрешенных ресурсов для тестирования систем в процессе работы;
- Компьютеры, ноутбуки, планшеты и прочие устройства, за исключением устройств, предоставленных площадкой;
- Периферийные устройства (клавиатуры, манипуляторы типа мышь и прочие устройства) за исключением устройств, предоставленных площадкой.

Задание для демонстрационного экзамена по комплекту оценочной документации № 1.2 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

(образец)

Задание включает в себя следующие разделы:

1. Формат Демонстрационного экзамена
2. Формы участия
3. Вид аттестации
4. Модули задания, критерии оценки и необходимое время
5. Необходимые приложения

Продолжительность выполнения задания: 5,5 ч.

8. Формат Демонстрационного экзамена:

Очный

9. Форма участия:

Индивидуальная

10. Вид аттестации:

ГИА

11. Модули задания, критерии оценки и необходимое время

Модули и время сведены в Таблице 1.

Таблица 1.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
1.	1. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	A. Организация работы и управление B. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	2,5 часа	1. 2. 5.	0	15,3	15,3
2.	2. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	C. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	3 часа	2. 5.	0	12,7	12,7
				Итого		28	28

Модули с описанием работ

Модуль 1: Технологии анализа и защиты сетевого трафика, установка и конфигурирование

Описание

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.

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

Доступы и прочие данные указаны в дополнительной карточке задания

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

Задание 1: настройка сетевого окружения и компонентов систем

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 или Bridge, или сеть NAT для виртуального «Интернета» (в соответствии с инфраструктурой площадки, для связи всех координаторов между собой)

При работе на сервере виртуализации данные могут отличаться. Также при работе на сервере допускается создание дополнительной сети для обмена файлами, дистрибутивами, ключами между всеми ВМ.

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

IP адреса защищенных сетей (пример):

Центральный офис «Сеть 1 ЦО»: 192.168.100.0/24

Офис филиал «Сеть 1 Филиал»: 192.168.200.0/25

Офис сеть 2 «Сеть 2 Офис»: 172.16.2.0/26

Общий «Интернет» для всех координаторов: 10.20.30.0/27

Адреса выбираются самостоятельно из указанного диапазона.

Необходимо записать адреса, логины и пароли в текстовый файл vpn.txt.

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

Также могут понадобиться дополнительные компоненты, находящиеся в каталогах дистрибутивов.

Задание 1.1. Установка ПО Vpn Administrator для создания защищённой сети:

Установить СУБД на виртуальную машину WSRV-DB. При установке необходимо использовать смешанную аутентификацию (пользователь sa). Пароль БД установить 12345678.

Установить и настроить рабочее место администратора VPN (на базе виртуальной машины WSRV-NCC-1): Центр управления сетью (серверное и клиентское приложение ЦУС и УКЦ. Использовать ранее установленную базу данных на отдельном сервере.

Верным выполнением задания является установка базы данных на отдельный сервер.

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 на соответствующие виртуальные машины:

установить ПО VPN Client, рабочее место администратора;

Рабочее место администратора должно быть защищено токеном аутентификации. Необходимо настроить вход в систему по токену (ключу). Парольный вход должен быть отключен.

установить ПО VPN Coordinator;

установить ПО VPN Coordinator;

установить ПО VPN Client, рабочее место пользователя;

Необходимо зафиксировать процесс установки только скриншотами изменяемых вручную форм и скриншот первого запуска приложения.

Задание 1.3. Защита локально-вычислительной сети предприятия с применением ПО VPN

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.

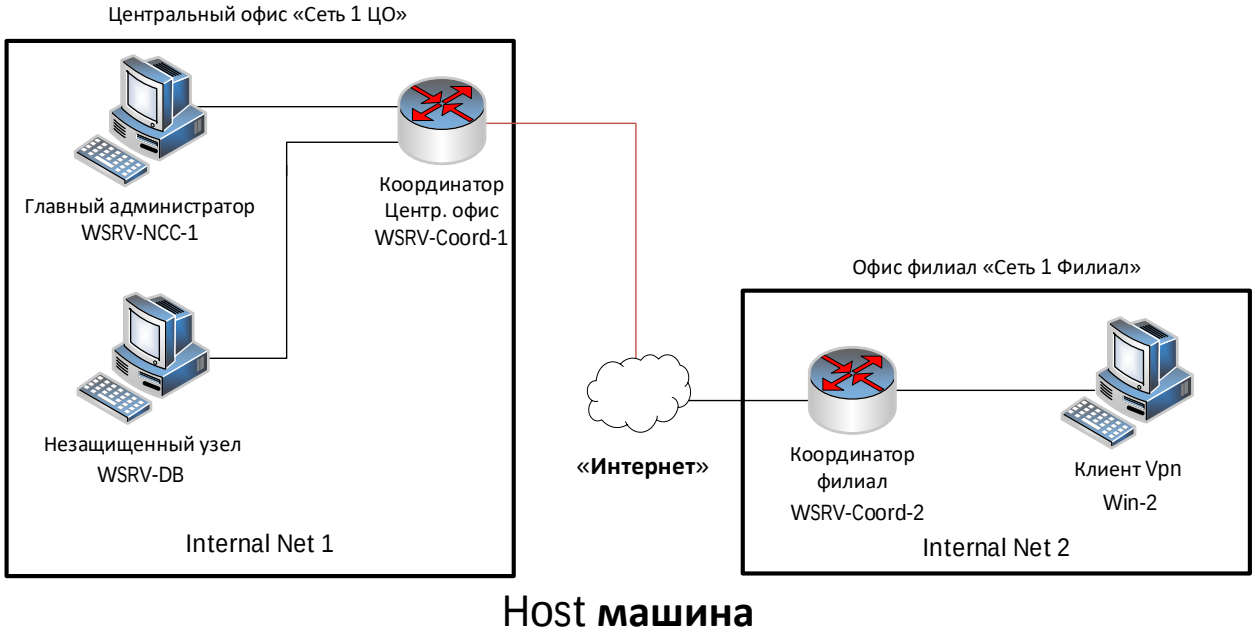


Рисунок 1 Схема защищенной сети

В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети и связи между ними (см. таблицу 1 и таблицу 2).

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

Вирт. машина	**Название сетевого узла**	**ПО Vpn**	**ОС сетевого узла**	**Имя пользователя сетевого узла, уровень полномочий**
WSRV-NCC-1	Главный администратор (VM) (защита токеном)	Vpn Administrator (ЦУС клиент и сервер + УКЦ) Vpn Client	ОС Server	Admin (защита токеном)
WSRV-DB	База данных (незащищенный узел)	—	ОС Server	—
WSRV-Coord-1	Координатор Центр Офис (VM)	Vpn Coordinator	ОС Server	CoordinatorOffice
WSRV-Coord-2	Координатор Филиал (VM)	Vpn Coordinator	ОС Server	CoordinatorSub

Win-2	Пользователь_2 Филиал (VM)	Vpn Client	ОС Pro	User2, минимальные полномочия

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	CoordinatorOffice	Admin	CoordinatorSub	user02
CoordinatorOffice	×	*	*	
Admin	*	×		*
CoordinatorSub	*		×	*
user02		*	*	×

Задание 1.4. 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, поменять тип паролей для пользователей («собственный»). Задать пароли пользователей и сохранить в текстовый файл. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить в папку на рабочем столе).

Создать группы узлов для центрального офиса 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 (на координаторах 2 интерфейса – внешний и внутренний), проверить доступность соседних узлов.

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

Стоит напомнить, что место администратора должно быть защищено токеном.

Задание 1.5. Модификация структуры защищенной сети

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

Модификация структуры сети:

- Добавить новый сетевой узел user01 и пользователя user01 за координатором ЦентрОфис (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем user02. На указанных узлах проверить появление нового узла.
- Добавить пользователя user02 на узле Пользователь_2 Филиал (Win-2 филиала), связать его со всеми пользователями группы узлов центральный офис и филиал. Для указанных пользователей проверить появление новой связи.
- Войти в Vpn клиент от данного пользователя на узле филиала.
- Отправить сообщение пользователю user01 с узла admin.
- зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:

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

Модуль 2: Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование

Задание 2.1. Компрометация узла защищенной сети

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя.

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

- скомпрометировать ключи пользователя user02 на узле Пользователь_2 Филиал
- произвести смену ключей пользователя и сетевых узлов,
- отправить обновления и произвести процедуру смены ключа пользователя на узле Пользователь_2 Филиал (фиксировать все шаги),
- войти от данного пользователя на узле филиала,
- проверить работу защищенной сети после обновления отправив сообщение от пользователя user02 администратору.

Восстановление взаимодействия с помощью ручной установки DST засчитано не будет.

Необходимо зафиксировать процесс настройки скриншотами или иным указанным способом.

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

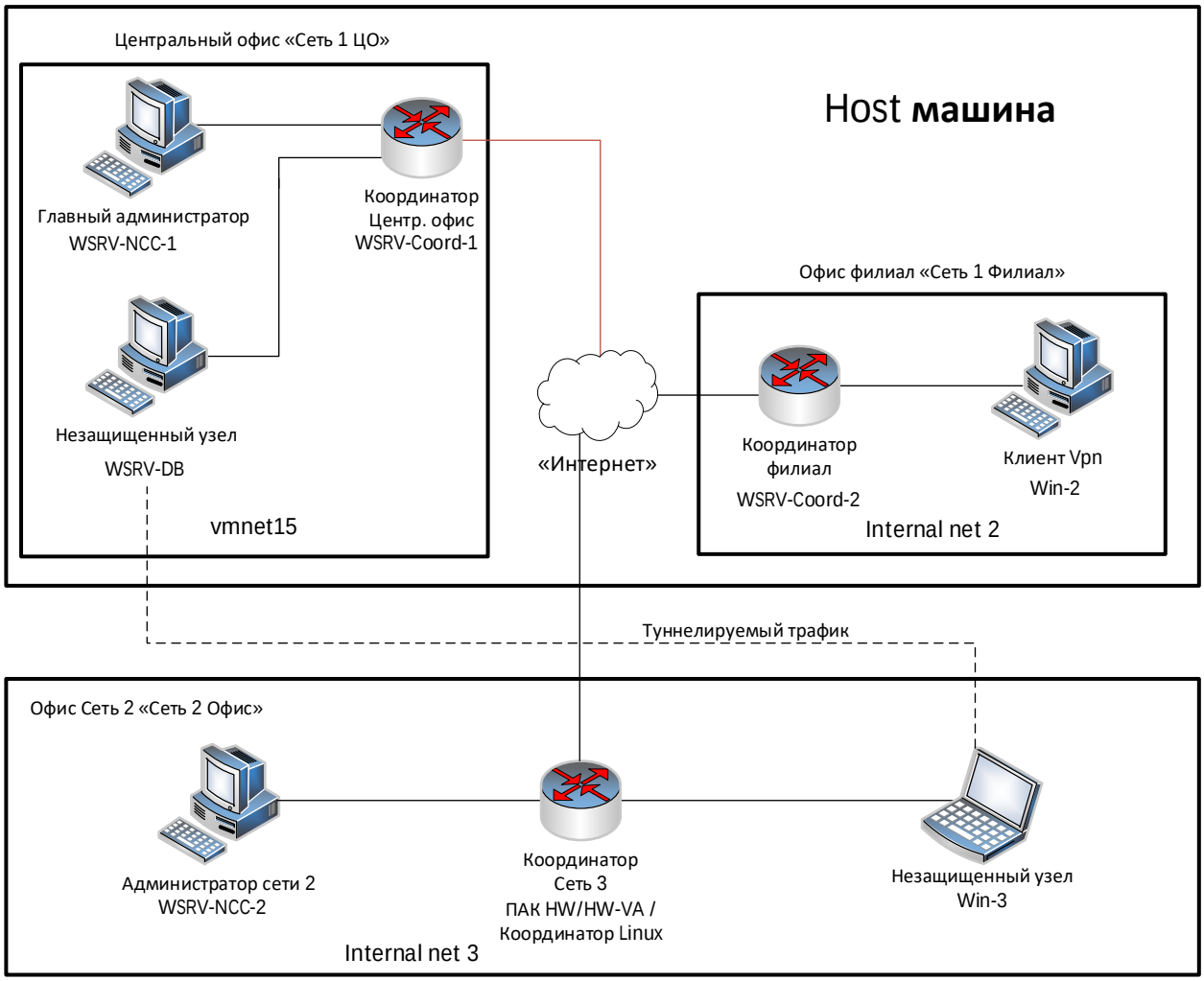


Рисунок 2 Схема межсетевого взаимодействия

Развернуть на WSRV-NCC-2 (Офис сеть 2 «Сеть 2 Офис») на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети:

- Рабочее место администратора (БД, ЦУС, УКЦ, Vpn Client)
- 1 координатор (ПАК HW или HV-VA, или координатор Linux в соответствии со структурой площадки). Допускается развертывание координатора windows (самостоятельным копированием виртуальной машины), но инициализация системы засчитана не будет.
- 1 узел Admin и пользователь Admin

Все пароли пользователей в сети Vpn сделать 12345678

Все пароли администраторов в сети Vpn сделать 12345678.

- Запустить координатор сети 2, настроить сеть в соответствии с заданием
- Настроить межсетевое между двумя защищёнными сетями взаимодействие с использованием асимметричного межсетевого мастер-ключа, сделать скриншоты всех этапов установки межсетевого взаимодействия.
- Проверить взаимодействие узлов, отправив сообщение узла Admin (сеть 1) на Admin (сеть 2).

Необходимо предоставить:

Файлы HTML структуры защищенной сети для обеих сетей после выполнения задания, скриншоты

Задание 2.3. Туннелирование в рамках межсетевого взаимодействия

- Подключить незащищенную машину в сети 3 (Win-3, без ПО Vpn).
- Для второй открытой машины использовать WSRV-DB в сети 1
- Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по шифрованному каналу. Проверить доступность незащищённых машин друг другу с помощью ICMP (ping), а также любым другим протоколом, например smb; проанализировать журналы IP-пакетов на координаторах.

Предоставить скриншоты выполнения.

5. Необходимые приложения

Приложение 1 Пояснения по подготовке площадки (документ docx)

Приложение 2 Карточка настроек сети и оборудования (документ docx)

Примерный план работы[1] Центра проведения демонстрационного экзамена по КОД № 1.2 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

	Примерное время	Мероприятие
Подготовительный день	08:00	Получение главным экспертом задания демонстрационного экзамена
	08:00 – 09:00	Проверка готовности проведения демонстрационного экзамена, заполнение Акта о готовности площадки
	09:00 – 09:15	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение протоколов
	09:15 – 09:30	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах
	09:30 – 09:45	Регистрация участников демонстрационного экзамена
	09:45 – 10:15	Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	10:15 – 12:00	Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение протоколов
	12:00 – 16:00	Подготовка и/или проверка работоспособности площадки в соответствии с заданием
День 1	08:45 – 09:00	Ознакомление с заданием и правилами
	09:00 – 09:15	Брифинг
	09:15 – 10:45	Выполнение модуля 1
	10:45 – 11:00	Перерыв, обработка помещения, проветривание
	11:00 – 12:00	Выполнение модуля 1
	12:00 – 12:45	Обед, обработка помещения, проветривание
	12:45 – 14:15	Выполнение модуля 2
	14:15 – 14:30	Перерыв, обработка помещения, проветривание
	14:30– 16:00	Выполнение модуля 2
	16:00 – 18:00	Работа экспертов, заполнение форм и оценочных ведомостей
	18:00 – 19:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола Подготовка площадки для следующей экзаменационной группы (при наличии)

[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.

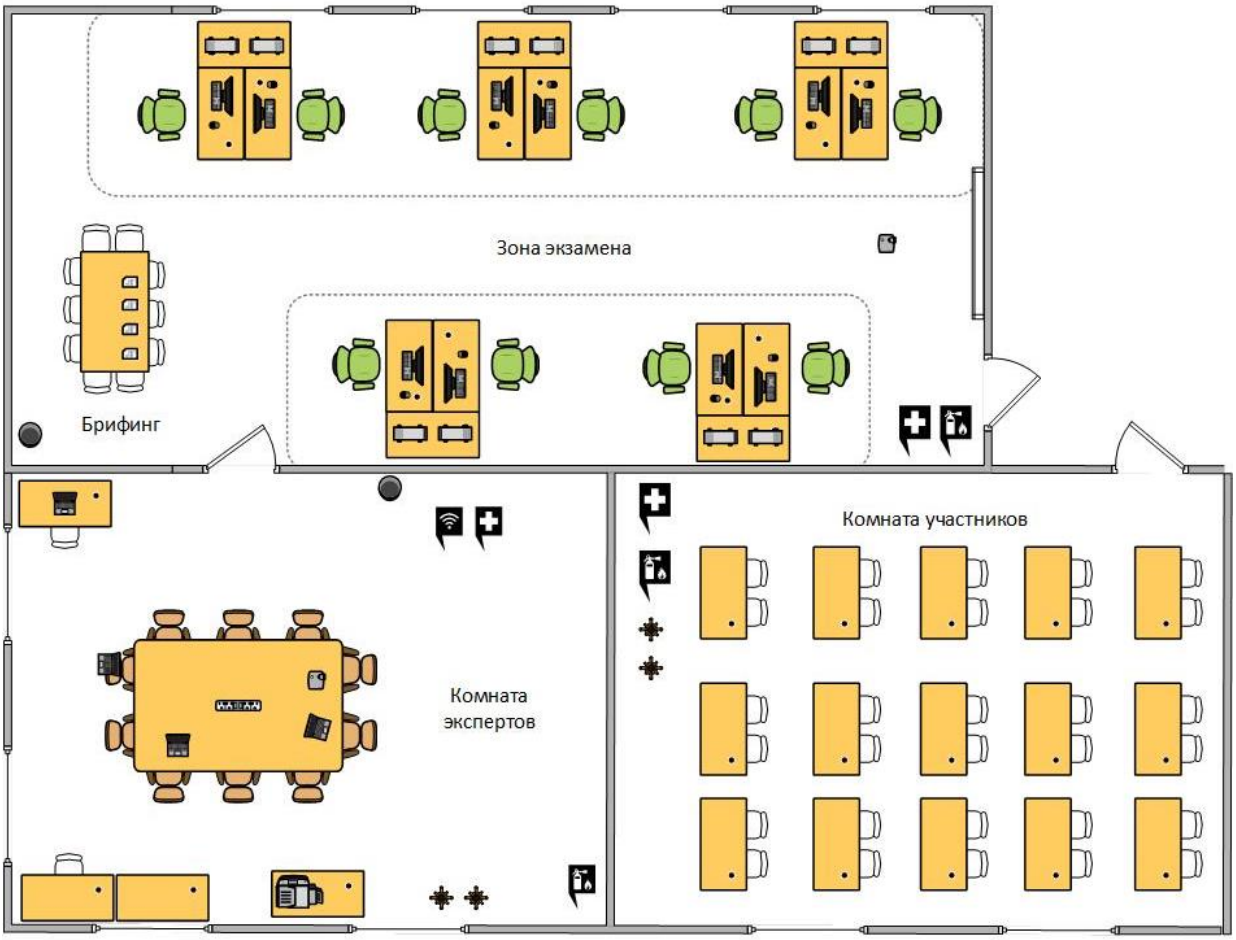
План застройки площадки для проведения демонстрационного экзамена по КОД № 1.2 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Номер компетенции: F7

Название компетенции: Корпоративная защита от внутренних угроз информационной безопасности

Общая площадь площадки: 100 м^2

План застройки площадки:



Приложения

Инфраструктурный лист для КОД № 1.2 (документ xlsx)

Пояснения по подготовке площадки для КОД № 1.2 (документ docx)

Карточка настроек сети и оборудования для КОД № 1.2 (документ docx)

Комплект оценочной документации № 1.3 для Демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

СОДЕРЖАНИЕ

Паспорт комплекта оценочной документации (КОД) № 1.3 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Комплект оценочной документации (КОД) № 1.3 разработан в целях организации и проведения демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» и рассчитан на выполнение заданий продолжительностью 3,5 часов.

КОД № 1.3 может быть рекомендован для оценки освоения основных профессиональных образовательных программ и их частей, дополнительных профессиональных программ и программ профессионального обучения, а также на соответствие уровням квалификации согласно Таблице (Приложение).

1. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации № 1.3 (Таблица 1).

Таблица 1.

Раздел WSSS	Наименование раздела WSSS	Важность (%)
1	**Организация работы и управление**	**3**
2	**Установка, конфигурирование и устранение неисправностей**	**6,7**
4	**Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**	**15,2**
6	**Технологии агентского мониторинга**	**8,5**
7	**Анализ выявленных инцидентов. Подготовка отчетов, классификация угроз и инцидентов**	**1,6**

Таблица 2.

Раздел WSSS	Наименование раздела WSSS
1.	Организация работы и управление
	Специалист должен знать и понимать: • Понимание принципов работы специалиста по информационной безопасности и их применение; • Знание принципов и положений безопасной работы в общем и по отношению к корпоративной среде;

	• Регламентирующие документы в области безопасности информационных систем; • Регламентирующие документы в области охраны труда и безопасности жизнедеятельности; • Важность организации труда в соответствии с методиками; • Методы и технологии исследования; • Важность управления собственным профессиональным развитием; • Скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню. • Важность умения слушать собеседника как части эффективной коммуникации; • Роли и требования коллег, и наиболее эффективные методы коммуникации; • Важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими; • Способы разрешения непонимания и конфликтующих требований; • Методы управления стрессом и гневом для разрешения сложных ситуаций.
	Специалист должен уметь: • Поддерживать безопасную, аккуратную и эффективную рабочую зону; • Использовать все оборудование и программное обеспечение безопасно и в соответствии с инструкциями производителя; • Следовать предписаниям в области охраны труда и безопасности жизнедеятельности; • Регулярно планировать свою работу и корректировать планы в соответствии с изменяющимися приоритетами; • Поддерживать рабочее место в должном состоянии и порядке. • Демонстрировать развитые способности слушать и задавать вопросы для более глубокого понимания сложных ситуаций; • Выстраивать эффективное письменное и устное общение; • Понимать изменяющиеся требования и адаптироваться к ним;
2.	Установка, конфигурирование и устранение неисправностей
	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 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 Windows Server и Linux Red Hat Enterprise Linux; • 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;
4.	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз
	Специалист должен знать и понимать: • Технологии работы с политиками информационной безопасности; • Создание новых политик, модификация существующих; • Общие принципы при работе интерфейсом системы защиты корпоративной информации; • Объекты защиты, персоны; • Ключевые технологии анализа трафика; • Типовые протоколы и потоки данных в корпоративной среде, такими как: • корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4) • веб-почта; • Интернет-ресурсы: сайты, блоги, форумы и т. д. (протоколы HTTP, HTTPS); • социальные сети; • интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP; • принтеры: печать файлов на локальных и сетевых принтерах; • любые съемные носители и устройства; • Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек; • Типы угроз информационной безопасности, типы инцидентов, • Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации; • Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации; • Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных; • Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации; • Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки; • Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе; • Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов; • Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации;
	Специалист должен уметь: • Создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты; • Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; • Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; • Работа со сводками, виджетами, сводками; • Работа с персонами;

	• Работа с объектами защиты; • Провести имитацию процесса утечки конфиденциальной информации в системе; • Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; • Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. • Работа с категориями и терминами; • Использование регулярных выражений; • Использование морфологического поиска; • Работа с графическими объектами; • Работа с выгрузками и баз данных; • Работа с печатями и бланками; • Работа с файловыми типами; • Эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;
6.	Технологии агентского мониторинга
	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.
	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.
7.	Анализ выявленных инцидентов. Подготовка отчетов, классификация угроз и инцидентов
	Специалист должен знать и понимать: • Основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах; • Инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз; • Типовой пакет нормативных документов, необходимого для развёртывания и эксплуатации системы корпоративной защиты в организации; • Виды типовых отчетных форм о выявленных угрозах и инцидентах; • Типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации; • Понимать подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз;

	• Системы DLP и требования по информационной безопасности. • Категорирование информации в РФ. • Юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; Специальные технические средства • Меры по обеспечению юридической значимости DLP (Pre-DLP). • Практику право применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (Post-DLP).
	Специалист должен уметь: • Разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности; • Проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации; • Создавать отчёты о выявленных инцидентах, угрозах и т.п. Представлять отчёты руководству, обосновывать полученные результаты анализа.

2. Формат Демонстрационного экзамена:

Очный

3. Форма участия:

Индивидуальная

4. Вид аттестации:

Промежуточная

5. Обобщенная оценочная ведомость.

В данном разделе определяются критерии оценки и количество начисляемых баллов (судейские и объективные) (Таблица 3).

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 35.

Таблица 3.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
1.	1. Установка и конфигурирование компонентов DLP системы	A. Организация работы и управление B. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	0,5 часа	1, 2	0	9,70	9,70
2.	2. Технологии агентского мониторинга	C. Технологии агентского мониторинга	1 час	6	0	8,50	8,50
3.	3. Разработка и применение политик, анализ выявленных инцидентов	D. Разработка политик безопасности, анализ выявленных инцидентов	2 часа	4, 7	0	16,80	16,80
				Итого		35	35

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

6.1. Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» — 3 чел.

6.2. Расчет количества экспертов исходя из количества рабочих мест и участников осуществляется по схеме согласно Таблице 4:

Таблица 4.

Количество постов-рабочих мест / Количество участников	1-5	6-10	11-15	16-20	21-25
От 1 до 5	3				
От 6 до 10		3			
От 11 до 15			4		
От 16 до 20				5	
От 21 до 25					6

7. Список оборудования и материалов, запрещенных на площадке

- Мобильные телефоны, смартфоны, рации, беспроводные, проводные наушники и другие средства связи;
- Собственные заметки, шпаргалки, книги и прочие документы;
- Личная электронная почта, мессенджеры и прочие средства связи посредством сети Интернет за исключение разрешенных ресурсов для тестирования систем в процессе работы;
- Компьютеры, ноутбуки, планшеты и прочие устройства, за исключением устройств, предоставленных площадкой;
- Периферийные устройства (клавиатуры, манипуляторы типа мышь и прочие устройства) за исключением устройств, предоставленных площадкой.

Задание для демонстрационного экзамена по комплекту оценочной документации № 1.3 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

(образец)

Задание включает в себя следующие разделы:

1. Формат Демонстрационного экзамена
2. Формы участия
3. Вид аттестации
4. Модули задания, критерии оценки и необходимое время
5. Необходимые приложения

Продолжительность выполнения задания: 3,5 ч.

1. Формат Демонстрационного экзамена:

Очный

2. Форма участия:

Индивидуальная

3. Вид аттестации:

Промежуточная

4. Модули задания, критерии оценки и необходимое время

Модули и время сведены в Таблице 1.

Таблица 1.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
1.	1. Установка и конфигурирование компонентов DLP системы	A. Организация работы и управление B. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	0,5 часа	1, 2	0	9,70	9,70
2.	2. Технологии агентского мониторинга	C. Технологии агентского мониторинга	1 час	6	0	8,50	8,50
3.	3. Разработка и применение политик, анализ выявленных инцидентов	D. Разработка политик безопасности, анализ выявленных инцидентов	2 часа	4, 7	0	16,80	16,80
				Итого		35	35

Модули с описанием работ

Модуль 1: Установка и конфигурирование компонентов DLP системы

Введение

В компания «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 носители информации, электронная почта и различные интернет-ресурсы.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены.

Подготовлены следующие виртуальные машины для дальнейшей работы:

AD Сервер с контроллером домена

DLP сервер установлен (но не настроен), активирована лицензия

Виртуальная машина сервера агентского мониторинга

Виртуальные машины «нарушителей»

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов. До установки системы необходимо подготовить доменных пользователей в соответствии с заданием.

Сетевые настройки указаны в дополнительных сведениях к заданию.

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными в соответствии с номером рабочего места (например, server-16).

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

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например: Задание_5_копирование.jpg.

Задание 1: Настройка контроллера домена

Необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: user1, пароль: 12345678, запретить локальный вход в систему

Логин: user2, пароль: 12345678, запретить локальный вход в систему

В случае проблем с настройкой допускается использовать стандартных пользователей из карточки задания, но не засчитывается.

Задание 2: Настройка DLP сервера

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

Необходимо вычислить IP-адрес сервера через локальную консоль виртуальной машины.

Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам.

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

Для входа в веб-консоль необходимо использовать ранее созданного пользователя домена с полными правами 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» с заголовком IWTM.

Корректно выполненным заданием будет являться работоспособная система с верно настроенными параметрами.

Задание 3: Проверка работоспособности сервера и клиента агентского мониторинга

Необходимо запустить и войти в консоль управления сервером агентского мониторинга.

Синхронизировать каталог пользователей и компьютеров с Active Directory.

Проверить соединение агента мониторинга с сервером агентского мониторинга.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» с заголовком IWDM.

Задание 4: Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)

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

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

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога.

Зафиксировать выполнение задания скриншотом настройки в web-консоли.

Стоит учесть, что неправильная настройка DNS на серверных машинах, а также неправильные настройки брандмауэра могут привести к неработоспособной системе сканирования сетевых ресурсов.

Задание 5: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания

событий) для данных, содержащих слово «Экзамен», установить низкий уровень угрозы для всех событий, добавить тег «Экзамен».

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

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена).

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Модуль 2: Технологии агентского мониторинга

Задания выполняются только с помощью компонентов DLP системы (не групповыми политиками или аналогичными решениями).

Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т.д. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т.д.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 2».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CP-1.jpg

где CP – сокращение от англ. creating a policy, 1 – номер задания

Пример 2 для сохранения скриншота работающей политики: PW-1.jpg

где PW – сокращение от англ. policy work, 1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики:

PW-1-2.jpg

где PW – сокращение от англ. policy work, 1 – номер задания; 2 – номер скриншота для задания 1.

Задание 1

Необходимо создать новую политику, применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику.

Зафиксировать выполнение скриншотом.

Задание 2

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

Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли с указанием адреса.

Задание 3

Для удаленного управления необходимо создать дополнительного локального офицера безопасности для доступа к серверу агентского мониторинга с полными правами на управление и просмотр разделов.

Имя пользователя: user1, пароль: 12345678

Проверить работоспособность с удаленной консоли, установленной ранее, зафиксировать выполнение скриншотом.

Задание 4

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 5

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 6

Необходимо поставить на контроль буфер обмена в текстовых процессорах.

Проверить работоспособность и зафиксировать выполнение занесением пары событий в веб-консоль DLP-сервера на любые политики. Также подтвердить выполнение скриншотом.

Задание 7

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Задание 8

Необходимо поставить на контроль печать документов на принтерах. Продемонстрировать работоспособность на любую из политик.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 9

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 15 секунд или при переходе на другую страницу.

Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в веб-консоли DLP-сервера. Подтвердить выполнение задания скриншотами.

Задание 10

Заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 11

На машине нарушителя необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Модуль 3: Разработка и применение политик, анализ выявленных инцидентов

Введение

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Для некоторых политик необходима работа с разными разделами консоли управления: категориями и терминами, технологиями, объектами защиты и т. п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, необходимо самостоятельно задать уровень угрозы).

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации с AD-сервером компании

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, т. к. легальные события не должны маркироваться как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Проверьте синхронизацию времени на всех системах, т. к. расхождение во времени между системами может повлиять на актуальность событий.

Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти в папке «Additional files» в общей папке из дополнительных сведений.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 3».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: 01-CP.jpg

где CP – сокращение от англ. creating a policy, 01 – номер задания

Пример 2 для сохранения скриншота работающей политики: 04-PW-1.jpg, 04-PW-2.jpg, где PW – сокращение от англ. policy work, 04 – номер задания, 1,2 – номер скриншотов

Задания на разработку политик можно выполнять в любом порядке.

ВНИМАНИЕ!

Необходимо называть политики / объекты / категории / теги и прочее ТОЛЬКО в соответствии с номером и названием задания

Политики — Политика X, например «Политика 4».

Для комбинированных политик формат: Политика 4.1, 4.2 и т.д.

Объект защиты — Объект X, например «Объект 11».

ВНИМАНИЕ!

Все политики «по умолчанию», находящиеся в консоли управления в процессе выполнения заданий должны быть отключены или удалены, так как могут помешать корректной оценке.

ВНИМАНИЕ!

При разработке и тестировании политик стоит учитывать, что нарушителем могут являться не только указанные в задании пользователи, а еще и виртуальная машина с агентом мониторинга.

ВНИМАНИЕ!

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.

Задание 1

Создайте локальную группу пользователей «Сотрудники под наблюдением». Добавьте в нее трех любых пользователей. Подтвердите выполнение задания скриншотами.

Задание 2

Для работы системы необходимо настроить периметр компании:

Почтовый домен: demo.lab.

Список веб ресурсов необходимо создать и назвать «Доверенные домены»: worldskills.org, filialdemo.lab, demolab-info.ru, dlpsystems.lab.

Группа персон 1: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Задание 3

Для недавно нанятого аудитора компании необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей без возможности редактирования. Области видимости: все.

Логин: auditor, пароль: 12345678

Подтвердите выполнение задания скриншотами.

Политика 4

В связи с секретностью при организации очередного WorldSkills, совет директоров решил контролировать передачу информации о WorldSkills за пределы компании. В связи с этим необходимо создать политику на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills».

Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять пробел между словами, например: «Ворлд Skills». Ложных срабатываний быть не должно (например, просто на Ворлд или Skills).

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: мобильники

Проверить работоспособность.

Политика 5

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%.

Для пустого документа:

Вердикт: разрешить √

Уровень нарушения: нет

Тег: договор

Для заполненного документа:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: договор

Проверить работоспособность.

Политика 6

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании, запрещая любую внешнюю передачу документов, содержащих заполненные бланках, при этом пустые бланки контролировать не нужно.

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 7

Для мониторинга движения официальных документов необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Политика 8

В компании происходит передача сообщений, содержащих специальные коды доступа к внутренней информационной системе. Все коды находятся в документе «Коды компании» (10 штук). Необходимо контролировать коды внутри компании, но запрещать передачу за пределы.

Передача кодов внутри компании:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: коды

Передача кодов за пределы компании:

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 9

Сотрудники отдела ИТ 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 отдела информатизации.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: база

Проверить работоспособность.

Политика 10

В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу. Необходимо отслеживать следующие термины: COVID, COVID-19, коронавирус, коронавирусная инфекция.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: вирус

Проверить работоспособность.

Политика 11

Для защиты персональных данных сотрудников необходимо запрещать всем, кроме отдела кадров передавать информацию, содержащую данные паспортов (в том числе и сканы/фото), а также СНИЛС и ИНН.

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: пдн

Проверить работоспособность.

Задание 12: Анализ инцидентов, обычные сводки

Создайте новую вкладку сводки в разделе «Сводка» под названием «Экзамен» и создайте в ней 4 виджета:

Динамика активности по событиям за последнюю неделю

Статистика по политикам за последние 7 дней

По типу событий: необработанные нарушения за три дня

По топ-нарушителям за текущий месяц.

Задание 13: Анализ инцидентов, специальные выборки

Необходимо создать новую вкладку в разделе «Сводка» под названием «Особые выборки» и добавить в нее виджеты:

Отображающий события с уровнем угрозы от низкого до высокого на правила копирования (внешние носители, печать) за последние 7 дней.

5. Необходимые приложения

Приложение 1 Пояснения по подготовке площадки (документ docx)

Приложение 2 Карточка настроек сети и оборудования (документ docx)

Приложение 3 Эталонные файлы для выполнения заданий (архив zip)

Приложение 4 Пример пользователей и групп для домена (документ csv)

Примерный план работы[1] Центра проведения демонстрационного экзамена по КОД № 1.3 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

	Примерное время	Мероприятие
Подготовительный день	08:00	Получение главным экспертом задания демонстрационного экзамена
	08:00 – 09:00	Проверка готовности проведения демонстрационного экзамена, заполнение Акта о готовности площадки
	09:00 – 09:15	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение протоколов
	09:15 – 09:30	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах
	09:30 – 09:45	Регистрация участников демонстрационного экзамена
	09:45 – 10:15	Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	10:15 – 12:00	Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение протоколов
	12:00 – 16:00	Подготовка и/или проверка работоспособности площадки в соответствии с заданием
День 1	08:45 – 09:00	Ознакомление с заданием и правилами
	09:00 – 09:15	Брифинг
	09:15 – 09:45	Выполнение модуля 1
	09:45 – 10:00	Перерыв, обработка помещения, проветривание
	10:00 – 11:00	Выполнение модуля 2
	11:00 – 11:15	Перерыв, обработка помещения, проветривание
	11:15 – 13:15	Выполнение модуля 3
	13:15 – 14:00	Обед, обработка помещения, проветривание
	14:00 – 16:30	Работа экспертов, заполнение форм и оценочных ведомостей
	16:30 – 18:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола Подготовка площадки для следующей экзаменационной группы (при наличии)

[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.

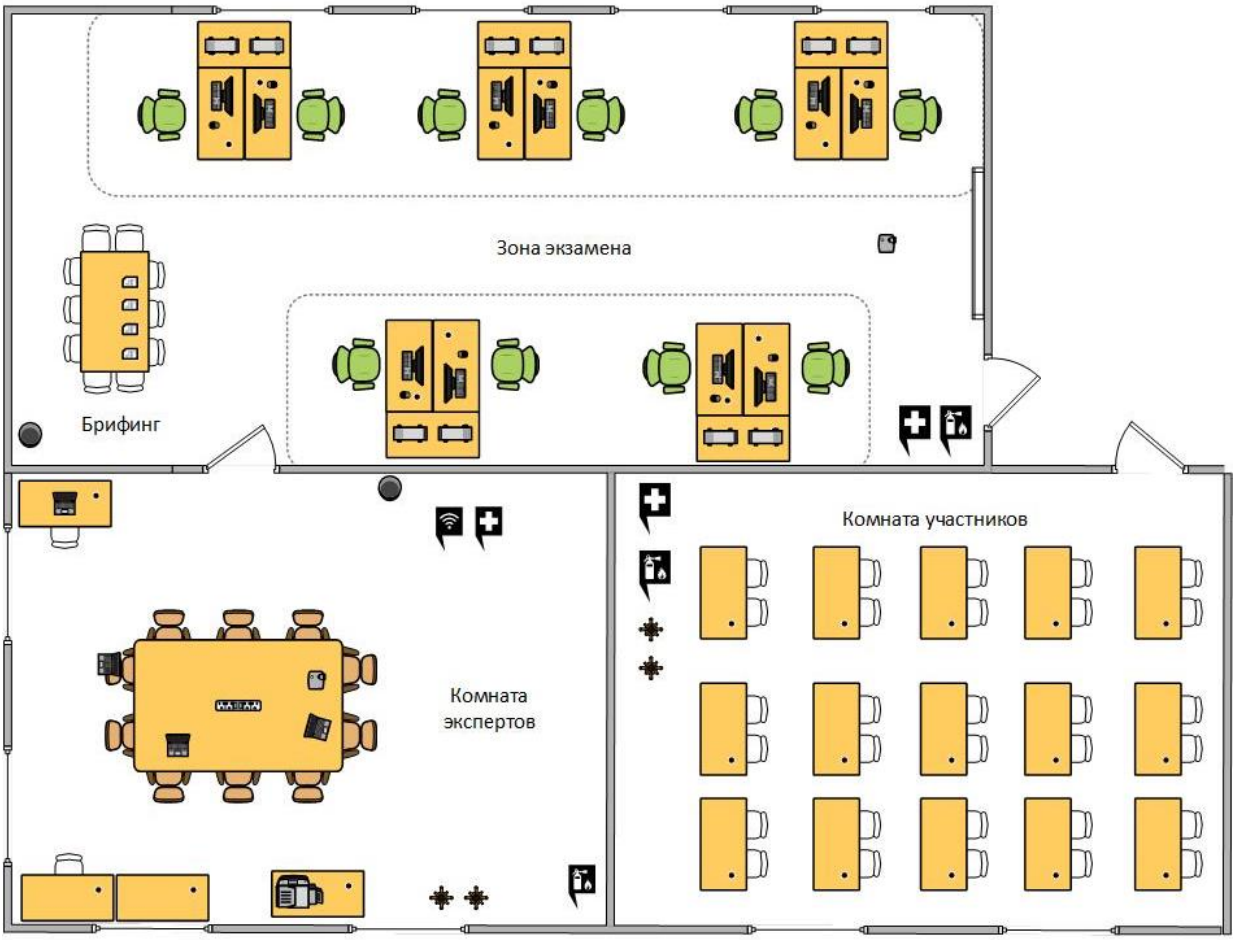
План застройки площадки для проведения демонстрационного экзамена по КОД № 1.3 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Номер компетенции: F7

Название компетенции: Корпоративная защита от внутренних угроз информационной безопасности

Общая площадь площадки: 100 м^2

План застройки площадки:



Приложения

Инфраструктурный лист для КОД № 1.3 (документ xlsx)

Пояснения по подготовке площадки для КОД № 1.3 (документ docx)

Карточка настроек сети и оборудования для КОД № 1.3 (документ docx)

Эталонные файлы для выполнения заданий для КОД № 1.3 (архив zip)

Пример пользователей и групп для домена (документ csv)

Комплект оценочной документации № 1.4 для Демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

СОДЕРЖАНИЕ

Паспорт комплекта оценочной документации (КОД) № 1.4 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Комплект оценочной документации (КОД) № 1.4 разработан в целях организации и проведения демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» и рассчитан на выполнение заданий продолжительностью 6 часов.

КОД № 1.4 может быть рекомендован для оценки освоения основных профессиональных образовательных программ и их частей, дополнительных профессиональных программ и программ профессионального обучения, а также на соответствие уровням квалификации согласно Таблице (Приложение).

1. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации № 1.4 (Таблица 1).

Таблица 1.

Раздел WSSS	Наименование раздела WSSS	Важность (%)
1	**Организация работы и управление**	**3**
2	**Установка, конфигурирование и устранение неисправностей**	**13,8**
4	**Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**	**20,6**
6	**Технологии агентского мониторинга**	**9,4**
7	**Анализ выявленных инцидентов. Подготовка отчетов, классификация угроз и инцидентов**	**2,2**

Таблица 2.

Раздел WSSS	Наименование раздела WSSS
1.	Организация работы и управление
	Специалист должен знать и понимать: • Понимание принципов работы специалиста по информационной безопасности и их применение; • Знание принципов и положений безопасной работы в общем и по отношению к корпоративной среде;

	• Регламентирующие документы в области безопасности информационных систем; • Регламентирующие документы в области охраны труда и безопасности жизнедеятельности; • Важность организации труда в соответствии с методиками; • Методы и технологии исследования; • Важность управления собственным профессиональным развитием; • Скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню. • Важность умения слушать собеседника как части эффективной коммуникации; • Роли и требования коллег, и наиболее эффективные методы коммуникации; • Важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими; • Способы разрешения непонимания и конфликтующих требований; • Методы управления стрессом и гневом для разрешения сложных ситуаций.
	Специалист должен уметь: • Поддерживать безопасную, аккуратную и эффективную рабочую зону; • Использовать все оборудование и программное обеспечение безопасно и в соответствии с инструкциями производителя; • Следовать предписаниям в области охраны труда и безопасности жизнедеятельности; • Регулярно планировать свою работу и корректировать планы в соответствии с изменяющимися приоритетами; • Поддерживать рабочее место в должном состоянии и порядке. • Демонстрировать развитые способности слушать и задавать вопросы для более глубокого понимания сложных ситуаций; • Выстраивать эффективное письменное и устное общение; • Понимать изменяющиеся требования и адаптироваться к ним;
2.	Установка, конфигурирование и устранение неисправностей
	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 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 Windows Server и Linux Red Hat Enterprise Linux; • 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;
4.	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз
	Специалист должен знать и понимать: • Технологии работы с политиками информационной безопасности; • Создание новых политик, модификация существующих; • Общие принципы при работе интерфейсом системы защиты корпоративной информации; • Объекты защиты, персоны; • Ключевые технологии анализа трафика; • Типовые протоколы и потоки данных в корпоративной среде, такими как: • корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4) • веб-почта; • Интернет-ресурсы: сайты, блоги, форумы и т. д. (протоколы HTTP, HTTPS); • социальные сети; • интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP; • принтеры: печать файлов на локальных и сетевых принтерах; • любые съемные носители и устройства; • Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек; • Типы угроз информационной безопасности, типы инцидентов, • Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации; • Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации; • Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных; • Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации; • Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки; • Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе; • Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов; • Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации;
	Специалист должен уметь: • Создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты; • Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; • Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; • Работа со сводками, виджетами, сводками; • Работа с персонами;

	• Работа с объектами защиты; • Провести имитацию процесса утечки конфиденциальной информации в системе; • Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; • Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. • Работа с категориями и терминами; • Использование регулярных выражений; • Использование морфологического поиска; • Работа с графическими объектами; • Работа с выгрузками и баз данных; • Работа с печатями и бланками; • Работа с файловыми типами; • Эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;
6.	Технологии агентского мониторинга
	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.
	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.
7.	Анализ выявленных инцидентов. Подготовка отчетов, классификация угроз и инцидентов
	Специалист должен знать и понимать: • Основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах; • Инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз; • Типовой пакет нормативных документов, необходимого для развёртывания и эксплуатации системы корпоративной защиты в организации; • Виды типовых отчетных форм о выявленных угрозах и инцидентах; • Типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации; • Понимать подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз;

	• Системы DLP и требования по информационной безопасности. • Категорирование информации в РФ. • Юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; Специальные технические средства • Меры по обеспечению юридической значимости DLP (Pre-DLP). Практику право применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (Post-DLP).
	Специалист должен уметь: • Разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности; • Проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации; • Создавать отчёты о выявленных инцидентах, угрозах и т.п. Представлять отчёты руководству, обосновывать полученные результаты анализа.

2. Формат Демонстрационного экзамена:

Дистанционный

3. Форма участия:

Индивидуальная

4. Вид аттестации:

ГИА

5. Обобщенная оценочная ведомость.

В данном разделе определяются критерии оценки и количество начисляемых баллов (судейские и объективные) (Таблица 3).

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 49.

Таблица 3.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
1.	1. Установка и конфигурирование компонентов DLP системы	A. Организация работы и управление B. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	1 час 45 минут	1, 2	0	16,80	16,80
2.	2. Технологии агентского мониторинга	C. Технологии агентского мониторинга	1 час 15 минут	6.	0	9,40	9,40
3.	3. Разработка и применение политик, анализ выявленных инцидентов	D. Разработка политик безопасности, анализ выявленных инцидентов	3 часа	4, 7	0	22,80	22,80
				Итого		49	49

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

6.1. Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» — 3 чел.

6.2. Расчет количества экспертов исходя из количества рабочих мест и участников осуществляется по схеме согласно Таблице 4:

Таблица 4.

Количество постов-рабочих мест / Количество участников	1-5	6-10	11-15	16-20	21-25
От 1 до 5	3				
От 6 до 10		3			
От 11 до 15			4		
От 16 до 20				5	
От 21 до 25					6

7. Список оборудования и материалов, запрещенных на площадке

- Мобильные телефоны, смартфоны, рации, беспроводные, проводные наушники и другие средства связи кроме случаев, когда мобильный телефон необходим для видеосвязи;
- Собственные заметки, шпаргалки, книги и прочие документы;
- Личная электронная почта, мессенджеры и прочие средства связи посредством сети Интернет за исключение разрешенных ресурсов для тестирования систем в процессе работы;
- Компьютеры, ноутбуки, планшеты и прочие устройства, за исключением устройств, предоставленных площадкой кроме случаев, когда планшет или ноутбук необходим для видеосвязи;

Задание для демонстрационного экзамена по комплекту оценочной документации № 1.4 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

(образец)

Задание включает в себя следующие разделы:

1. Формат Демонстрационного экзамена
2. Формы участия
3. Вид аттестации
4. Модули задания, критерии оценки и необходимое время
5. Необходимые приложения

Продолжительность выполнения задания: 6 ч.

1. Формат Демонстрационного экзамена:

Дистанционный

2. Форма участия:

Индивидуальная

3. Вид аттестации:

ГИА

4. Модули задания, критерии оценки и необходимое время

Модули и время сведены в Таблице 1.

Таблица 1.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
4.	1. Установка и конфигурирование компонентов DLP системы	A. Организация работы и управление B. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	1 час 45 минут	1, 2	0	16,80	16,80
5.	2. Технологии агентского мониторинга	C. Технологии агентского мониторинга	1 час 15 минут	6.	0	9,40	9,40
6.	3. Разработка и применение политик, анализ выявленных инцидентов	D. Разработка политик безопасности, анализ выявленных инцидентов	3 часа	4, 7	0	22,80	22,80
				Итого		49	49

Модули с описанием работ

Модуль 1: Установка и конфигурирование компонентов DLP системы

Введение

В компания «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 носители информации, электронная почта и различные интернет-ресурсы.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены.

Подготовлены следующие виртуальные машины для дальнейшей работы:

AD Сервер с контроллером домена

DLP сервер установлен (но не настроен), активирована лицензия

Виртуальная машина для установки сервера агентского мониторинга

Виртуальные машины «нарушителей» для установки агентов

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов. До установки системы необходимо подготовить доменных пользователей в соответствии с заданием.

Сетевые настройки указаны в дополнительных сведениях к заданию.

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными в соответствии с номером рабочего места (например, server-16).

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

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например: Задание_5_копирование.jpg.

Для отправки скриншотов и отчетов необходимо использовать систему, обозначенную экспертами в подготовительный день, данные могут быть указаны в дополнительной карточке задания.

Задание 1: Настройка контроллера домена

Необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: user1, пароль: 12345678, запретить локальный вход в систему

Логин: user2, пароль: 12345678, запретить локальный вход в систему

Логин: user3, пароль: 12345678, права администратора домена и локального администратора

Логин: user4, пароль 12345678, права пользователя домена

Задание 2: Настройка DLP сервера

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

Необходимо вычислить IP-адрес сервера через консоль виртуальной машины или иным способом, обозначенным экспертами.

Настроить DNS на сервере для корректной работы.

Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам.

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

Для входа в веб-консоль необходимо использовать ранее созданного пользователя домена с полными правами 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» с заголовком IWTM.

Корректно выполненным заданием будет являться работоспособная система с верно настроенными параметрами.

Файлы отчетов необходимо отправить в соответствии с требованиями в дополнительной карточке задания или в соответствии с требованиями экспертов.

Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить базу данных с паролем суперпользователя 12345678.

Установить сервер агентского мониторинга с параметрами по умолчанию.

При установке необходимо установить соединение с DLP-сервером контроля сетевого трафика по IP-адресу и токену, но можно сделать это и после установки сервера агентского мониторинга.

Настроить пользователя консоли управления: officer с паролем 12345678.

Синхронизировать каталог пользователей и компьютеров с Active Directory.

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

Зафиксировать факт создания пользователя и настройку скриншотом.

Проверить работоспособность входа в консоль управления без ввода пароля. Стоит обратить внимание, что если сервер не введен в домен, данная опция работать не будет.

Зафиксировать факт подключения без пароля скриншотом.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» с заголовком IWDM.

Файлы отчетов необходимо отправить в соответствии с требованиями в дополнительной карточке задания или в соответствии с требованиями экспертов.

Задание 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить агент мониторинга с помощью задачи первичного распространения с сервера агентского мониторинга. Необходимо учесть, что установка осуществляется только с правами администратора (доменного или локального). Ручная установка с помощью создания пакета установки является неверным выполнением задания.

Зафиксировать успешное выполнение задачи скриншотом.

В случае проблем стоит проверить настройки брандмауэра и DNS, а также проверить настройки в дополнительной карточке задания.

Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)

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

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

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога.

Зафиксировать выполнение задания скриншотом настройки в web-консоли.

Стоит учесть, что неправильная настройка DNS на серверных машинах, а также неправильные настройки брандмауэра могут привести к неработоспособной системе сканирования сетевых ресурсов.

Задание 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания событий) для данных, содержащих слово «Экзамен», установить низкий уровень угрозы для всех событий, добавить тег «Экзамен».

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

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена).

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задание 7: Защита системы с помощью сертификатов

Создайте цифровой сертификат (дерево сертификатов) формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности, длине ключа 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)

сертификат сервиса (веб-сайта)

Итоговый результат должен включать:

Дерево из 2 (3)-х сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов.

Содержимое команд по генерации ключей и сертификатов в текстовом файле «отчет.txt»

Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе просмотра сертификатов Windows (закладки «Общие», «Путь сертифкации»).

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

Генерацию сертификатов зафиксируйте скриншотами.

Для отправки скриншотов и отчетов необходимо использовать систему, обозначенную экспертами в подготовительный день, данные могут быть указаны в дополнительной карточке задания.

Модуль 2: Технологии агентского мониторинга

Задания выполняются только с помощью компонентов DLP системы (не групповыми политиками или аналогичными решениями).

Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т.д. в соответствии с заданием, например, «Политика 1» или «Правило 1.2» и т.д.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 2».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CP-1.jpg

где CP – сокращение от англ. creating a policy,

1 – номер задания

Пример 2 для сохранения скриншота работающей политики: PW-1.jpg

где PW – сокращение от англ. policy work,

1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики: PW-1-2.jpg

где PW – сокращение от англ. policy work,

1 – номер задания;

2 – номер скриншота для задания 1.

Для отправки скриншотов и отчетов необходимо использовать систему, обозначенную экспертами в подготовительный день, данные могут быть указаны в дополнительной карточке задания.

Задание 1

Необходимо создать новую политику, применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику.

Зафиксировать выполнение скриншотом.

Задание 2

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

Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли с указанием адреса.

Задание 3

Для удаленного управления необходимо создать дополнительного локального офицера безопасности для доступа к серверу агентского мониторинга с полными правами на управление и просмотр разделов.

Имя пользователя: user1, пароль: 12345678

Проверить работоспособность с удаленной консоли, установленной ранее, зафиксировать выполнение скриншотом.

Задание 4

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 5

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 6

Необходимо поставить на контроль буфер обмена в текстовых процессорах.

Проверить работоспособность и зафиксировать выполнение занесением пары событий в веб-консоль DLP-сервера на любые политики. Также подтвердить выполнение скриншотом.

Задание 7

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Задание 8

Необходимо поставить на контроль печать документов на принтерах. Продемонстрировать работоспособность на любую из политик IWTM.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 9

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 15 секунд или при переходе на другую страницу.

Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в веб-консоли DLP-сервера. Подтвердить выполнение задания скриншотами.

Задание 10

Заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 11

На машине нарушителя необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 12

Необходимо установить (сменить) пароль для удаления агента мониторинга на машине нарушителя с помощью средств сервера агентского мониторинга (удаленно).

Проверить работоспособность и зафиксировать выполнение скриншотом

Модуль 3: Разработка и применение политик, анализ выявленных инцидентов

Введение

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Для некоторых политик необходима работа с разными разделами консоли управления: категориями и терминами, технологиями, объектами защиты и т. п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, необходимо самостоятельно задать уровень угрозы).

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации с AD-сервером компании

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, т. к. легальные события не должны маркироваться как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Проверьте синхронизацию времени на всех системах, т. к. расхождение во времени между системами может повлиять на актуальность событий.

Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти в папке «Additional files» в общей папке из дополнительных сведений.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 3».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: 01-CP.jpg

где CP – сокращение от англ. creating a policy, 01 – номер задания

Пример 2 для сохранения скриншота работающей политики: 04-PW-1.jpg, 04-PW-2.jpg, где PW – сокращение от англ. policy work, 04 – номер задания, 1,2 – номер скриншотов

Для отправки скриншотов и отчетов необходимо использовать систему, обозначенную экспертами в подготовительный день, данные могут быть указаны в дополнительной карточке задания.

Задания на разработку политик можно выполнять в любом порядке.

ВНИМАНИЕ!

Необходимо называть политики / объекты / категории / теги и прочее ТОЛЬКО в соответствии с номером и названием задания

Политики — Политика X, например, «Политика 4».

Для комбинированных политик формат: Политика 4.1, 4.2 и т.д.

Объект защиты — Объект X, например, «Объект 11».

ВНИМАНИЕ!

Все политики «по умолчанию», находящиеся в консоли управления в процессе выполнения заданий должны быть отключены или удалены, так как могут помешать корректной оценке.

ВНИМАНИЕ!

При разработке и тестировании политик стоит учитывать, что нарушителем могут являться не только указанные в задании пользователи, а еще и виртуальная машина с агентом мониторинга.

ВНИМАНИЕ!

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.

Задание 1

Создайте локальную группу пользователей «Сотрудники под наблюдением». Добавьте в нее трех любых пользователей. Подтвердите выполнение задания скриншотами.

Задание 2

Для работы системы необходимо настроить периметр компании:

Почтовый домен: demo.lab.

Список веб ресурсов необходимо создать и назвать «Доверенные домены»: worldskills.org, filialdemo.lab, demolab-info.ru, dlpsystems.lab.

Группа персон 1: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Задание 3

Для недавно нанятого аудитора компании необходимо создать пользователя системы IWTM с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей без возможности редактирования. Области видимости: все.

Логин: auditor, пароль: 12345678

Подтвердите выполнение задания скриншотами.

Политика 4

В связи с секретностью при организации очередного WorldSkills, совет директоров решил контролировать передачу информации о WorldSkills за пределы компании. В связи с этим необходимо создать политику на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills».

Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять пробел между словами, например: «Ворлд Skills». Ложных срабатываний быть не должно (например, просто на Ворлд или Skills).

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: мобильники

Проверить работоспособность.

Политика 5

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%.

Для пустого документа:

Вердикт: разрешить √

Уровень нарушения: нет

Тег: договор

Для заполненного документа:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: договор

Проверить работоспособность.

Политика 6

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании, запрещая любую внешнюю передачу документов, содержащих заполненные бланках, при этом пустые бланки контролировать не нужно.

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 7

Для мониторинга движения официальных документов необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Политика 8

В компании происходит передача сообщений, содержащих специальные коды доступа к внутренней информационной системе. Все коды находятся в документе «Коды компании» (8 штук). Необходимо контролировать коды внутри компании, но запрещать передачу за пределы.

Передача кодов внутри компании:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: коды

Передача кодов за пределы компании:

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 9

Ракетное вооружение для авиационных комплексов различного класса, в разработке которого участвует компания, планируется к внедрению в эксплуатацию. Информация о технике может иметь конфиденциальный и секретный характер, хотя и не содержать гриф.

Необходимо блокировать любые попытки передачи данных об этих объектах на внешние адреса. Технические объекты задаются буквенно-цифирными кодами на русском языке:

Р-Цифры-Буквы или РЦифрыБуквы или Р-ЦифрыБуквы

Р – русская буква «Р»

Цифры – не более 3-х подряд, например, 27 или 500 (обязательно наличие хотя бы одной цифры)

Буквы – от 2 до 3-х подряд, например, Р-27АЭ

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: ракеты

Проверить работоспособность.

Политика 10

Сотрудники отдела ИТ 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 отдела информатизации.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: база

Проверить работоспособность.

Политика 11

В связи с постоянными заказами на транспортировку больших грузов, сотрудники компании подрабатывают в тайне от начальства, занимаясь попутной перевозкой других грузов, а также пассажиров. В связи с этим необходимо отслеживать в почтовых сообщениях упоминания об автостопе, халтуре, подработке, грузовом такси.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: подработка

Проверить работоспособность.

Политика 12

Необходимо запретить передачу документов с грифом (информационной меткой) «ООО Demo Lab. Конфиденциально» или «ООО Demo Lab. Строго конфиденциально» любым сотрудникам за пределы компании. Обратите внимание, что при вводе информационной метки с клавиатуры сотрудники могут ошибаться и вводить между словами более 1 пробела или табуляции, а также писать название компании на русском языке, например, «ООО Demo Лаб», «ООО Демо Лаб».

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: печать

Проверить работоспособность.

Политика 13

В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу. Необходимо отслеживать следующие термины: COVID, COVID-19, коронавирус, коронавирусная инфекция.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: вирус

Проверить работоспособность.

Политика 14

Для защиты персональных данных сотрудников необходимо запрещать всем, кроме отдела кадров передавать информацию, содержащую данные паспортов (в том числе и сканы/фото), а также СНИЛС и ИНН.

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: пдн

Проверить работоспособность.

Политика 15

Необходимо контролировать передачу документов формата электронных таблиц (исключая csv файлы!), а также CAD-документации.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Задание 16: Анализ инцидентов, обычные сводки

Создайте новую вкладку сводки в разделе «Сводка» под названием «Экзамен» и создайте в ней 4 виджета:

Динамика активности по событиям за последнюю неделю

Статистика по политикам за последние 7 дней

По типу событий: необработанные нарушения за три дня

По топ-нарушителям за текущий месяц.

Задание 17: Анализ инцидентов, специальные выборки

Необходимо создать новую вкладку в разделе «Сводка» под названием «Особые выборки» и добавить в нее виджеты:

Отображающий события с уровнем угрозы от низкого до высокого на правила буфера обмена за последние 7 дней.

Отображающий события с любым одним тегом.

5. Необходимые приложения

Приложение 1 Пояснения по подготовке площадки (документ docx)

Приложение 2 Карточка настроек сети и оборудования (документ docx)

Приложение 3 Эталонные файлы для выполнения заданий (архив zip)

Приложение 4 Пример пользователей и групп для домена (документ csv)

Примерный план работы[1] Центра проведения демонстрационного экзамена по КОД № 1.4 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

	Примерное время	Мероприятие
Подготовительный день	08:00	Получение главным экспертом задания демонстрационного экзамена
	08:00 – 09:00	Проверка готовности проведения демонстрационного экзамена, заполнение Акта о готовности площадки
	09:00 – 09.25	Проверка подключения экспертов к системе видеосвязи
	09:25 – 09:45	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение протоколов
	09:45 – 10:00	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах
	10:00 – 10:15	Регистрация участников демонстрационного экзамена
	10:15 – 11:00	Проверка подключения участников к системам
	11:00 – 11:30	Инструктаж по работе в дистанционном формате
	11:30 – 13:00	Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении Проверка рабочих удаленных мест участников
	13:15 – 14:00	Перерыв
	14:00 – 15:00	Инструктаж участников о подключении к удаленной площадке, проверка связи, проверка рабочих мест участников на соответствие правилам ДЭ дистанционного формата
	15:00 – 16:30	Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение протоколов
	16:30 – 19:30	Подготовка и/или проверка работоспособности площадки в соответствии с заданием
День 1	08:00 – 08:30	Проверка подключения экспертов и участников к площадке
	08:30 – 09:00	Проверка рабочих мест участников
	09:00 – 09:30	Ознакомление с заданием и правилами
	09:30 – 10:00	Брифинг, подключение к площадке
	10:00 – 11:45	Выполнение модуля 1
	11:45 – 11:55	Перерыв
	11:55 – 13:10	Выполнение модуля 2

[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.

	13:10 – 14:00	Обед
	14:00 – 15:30	Выполнение модуля 3
	15:30 – 15:40	Перерыв
	15:40 – 17:10	Выполнение модуля 3
	17:10 – 19:10	Работа экспертов, заполнение форм и оценочных ведомостей
	19:10 – 20:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола Подготовка площадки для следующей экзаменационной группы (при наличии)

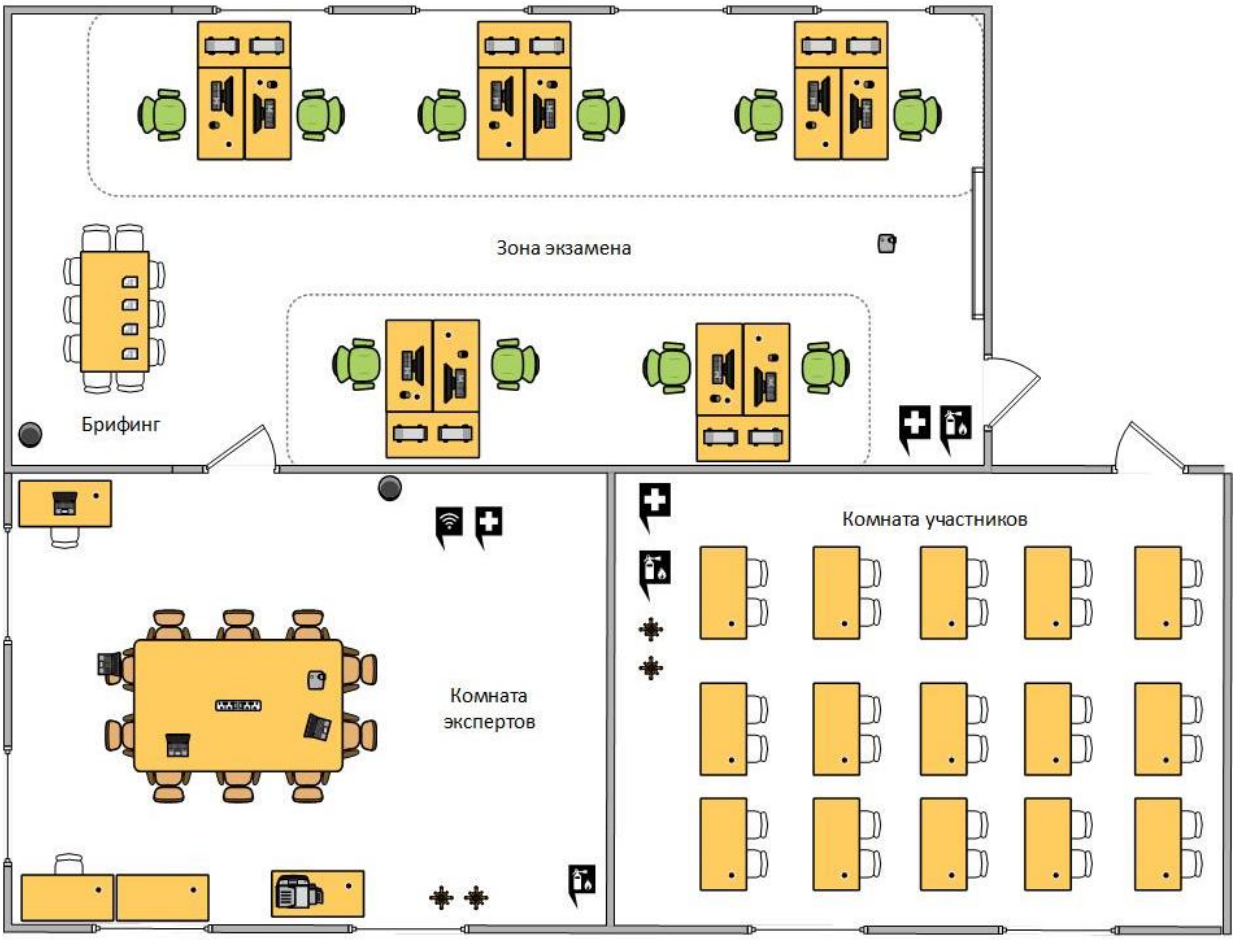
План застройки площадки для проведения демонстрационного экзамена по КОД № 1.4 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Номер компетенции: F7

Название компетенции: Корпоративная защита от внутренних угроз информационной безопасности

Общая площадь площадки: 100 м^2

План застройки площадки:



Приложения

Инфраструктурный лист для КОД № 1.4 (документ xlsx)

Особые условия проведения Демонстрационного экзамена в дистанционном / распределенном формате для КОД №1.4 (документ docx)

Приложение 1: Пояснения по подготовке площадки (документ docx)

Приложение 2: Карточка настроек сети и оборудования (документ docx)

Приложение 3: Эталонные файлы для выполнения заданий (архив zip)

Приложение 4: Пример пользователей и групп для домена (документ csv)

Приложение 5: Примерные схемы подключения к площадке (документ docx)

Приложение к КОД № 1.4
по компетенции №F7
«Корпоративная защита от внутренних угроз информационной безопасности»

Особые условия проведения Демонстрационного экзамена по стандартам Ворлдскиллс Россия в дистанционном / распределенном формате

Настоящие условия определяют порядок организации и проведения демонстрационного экзамена по компетенции №F7 «Корпоративная защита от внутренних угроз информационной безопасности» в соответствии с комплектом оценочной документации (КОД) № 1.4 в дистанционном / распределенном формате работы во время экзамена.

1. Технические средства, применяемые для организации и проведения демонстрационного экзамена

Условия видеотрансляции сдачи демонстрационного экзамена	Необходимо подключение участника в сервис видеоконференцсвязи на весь период проведения экзамена. Качество вывода трансляции должно быть не менее 1920×1080 точек не менее 5 кадров/с. Освещенность рабочего места должна быть достаточной для идентификации участника и проверки документов. Платформа для видеоконференцсвязи выдается организаторами или выбирается учреждением, рекомендованные: IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие.
Условия видеозаписи сдачи демонстрационного экзамена	Видеозапись должна осуществляться на сервисе видеоконференцсвязи и на локальном рабочем месте участника и загружаться по запросу экспертов на облачное хранилище. Качество записи должно быть не менее 1920×1080 точек не менее 10 кадров/с, битрейт не менее 3мбит/с, кодек H264 или h265 HEVC.
Условия трансляции экрана / рабочего места экзаменуемого	Качество вывода трансляции должно быть не менее 1920×1080 точек не менее 5 кадров/с, транслируется весь рабочий стол, допускается использование второго монитора для удобства работы (вывода окна с системой видеоконференцсвязи и/или файлов задания) с трансляцией второго экрана аналогично первому. Необходимо наличие веб-камеры для первоначальной идентификации участника и включения ее по запросу ГЭ или линейных экспертов. Допускается использование мобильных устройств для подключения камеры в случае отсутствия таковой на компьютере.
Условия записи экрана / рабочего места экзаменуемого	Для решения спорных моментов при проверке задания или прочих спорных моментов необходима локальная и/или облачная запись, качество записи должно быть не менее 1920×1080 точек не менее 10 кадров/с, битрейт не менее 3мбит/с, кодек H264 или h265 HEVC. При локальной записи

	рекомендуется использование OBS Studio и передача файла способом, оговоренным перед началом экзамена.
Условия передачи заданий демонстрационного экзамена экспертами участникам, а также результатов работы участниками экспертам	Сервисы видеоконференцсвязи (с помощью модулей чат и/или совместный доступ к документам; облачные хранилища с ограниченным доступом; распространение заданий напрямую главным экспертом при подключении к инфраструктуре площадки и использованием общего сетевого хранилища внутри площадки. Отправка отчетов и результатов работы (при необходимости) осуществляется таким же способом.
Условия демонстрации результата выполненной работы участниками экзамена	Участник выполняет работу также, как и на обычном демонстрационном экзамене, проверка осуществляется по результатам работы после окончания работы.
Дополнительное программное обеспечение необходимое для работы на ДЭ, включая программы совместной работы над документами, облачные хранилища, специфические программы необходимые для реализации задания ДЭ	Программы совместной работы выдаются либо организаторами, либо выбираются на усмотрение организации/главного эксперта в подготовительный день. Рекомендуемое ПО для записи/трансляции: OBS Studio последних версий, плагин VirtualCam для OBS Studio для вывода потока в качестве виртуальной веб-камеры.
Условия оказания помощи в установке и обучения работе с программным обеспечением, технической поддержки во время проведения ДЭ	Для помощи в установке ПО рекомендуется установить программу удаленной поддержки (например, TeamViewer). Технический эксперт площадки оказывает помощь в случае проблем с подключением, не связанных с качеством интернет-канала.

2. Особый план проведения демонстрационного экзамена (ПРИМЕР)

<table>
<tr><th rowspan="2">День</th><th rowspan="2">Примерное время</th><th colspan="2">Мероприятие</th></tr>
<tr><th>Действия экспертов</th><th>Действия участников экзамена</th></tr>
<tr><td></td><td colspan="3">Деятельность осуществляется согласно пункту 5 «Дополнительные условия», описанному в данном документе.
Электронные ресурсы указываются по выбору ГЭ/площадки проведения в подготовительные дни ДЭ</td></tr>
<tr><td rowspan="4">Подготовительный день С-1[1]</td><td colspan="3">Работа с экспертами ДЭ</td></tr>
<tr><td rowspan="3">08:00 – 08:30</td><td>1. Получение главным экспертом задания демонстрационного экзамена (далее ДЭ).</td><td rowspan="3">к работе не привлекаются</td></tr>
<tr><td>2. Работа в системе по проверке правильности внесенных данных.</td></tr>
<tr><td>3. Генерирование первичного протокола о блокировке схемы оценки из системы</td></tr>
</table>

[1] Если требуется, подготовка может начаться за несколько дней по проведения Демонстрационного экзамена

	08:30 – 08:50	1. Проверка оборудования и подключений Техническим экспертом / IT экспертом	к работе не привлекаются
		2. Проведение регистрации главным экспертом линейных экспертов ДЭ на выбранном электронном ресурсе: IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие 2.1. Тестирование экспертной группой работоспособности выбранных электронных ресурсов 2.2. Заполнение и загрузка документации экспертной группой	
		1. Оповещение главного эксперта о завершении и результатах проверки 2. Подтверждение Главным экспертом готовности	
	08:50 – 09:15	1. Проверка главным экспертом совместно с техническим администратором площадки готовность мест линейных экспертов к оценочной деятельности согласно инфраструктурному листу КОД 1.4 по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»	к работе не привлекаются
		2. Составление главным экспертом протокола о готовности мест экспертов к ДЭ	
	09:20 – 10:00	1. Проведение главным экспертом инструктажа Экспертной группы по охране труда и технике безопасности	к работе не привлекаются
		2. Ответы на вопросы линейных экспертов главным экспертом с использованием ресурсов IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие	
		3.1. Способ подписания электронный / скан (после согласования)	

		3.2. Используемые ресурсы IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие 3.3. Способ загрузки любой	
		3. Проверка главным экспертом подписей в Протоколе об ознакомлении с ТБ и ОТ экспертов с помощью ресурсов совместной работы.	
		4. Распределение главным экспертом обязанностей и судейских ролей по проведению ДЭ между членами Экспертной группы с помощью ресурсов IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие	
		5.1. Способ подписания электронный / скан (после согласования) 5.2. Используемые ресурсы IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие 5.3. Способ загрузки	
		5. Ознакомление линейных экспертов с правилами проведения ДЭ, оценки работ участников ДЭ в соответствии с заданием КОД 1.4 по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»	
		6. Подписание экспертами протокола блокировки критериев оценки: 6.1. Способ подписания — протокол согласия о подписи в электронной системе или печать и сканирование всех протоколов 5.4. Используемые ресурсы IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие 6.2. Способ загрузки любой	
		6. Распределение главным экспертом между линейными экспертами участников для осуществления контроля за	

		ходом выполнения ими задания ДЭ в соответствии с КОД 1.4 по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» – на одного линейного эксперта не более 4 участников. При достаточной квалификации экспертов возможно увеличение количества участников на 1 эксперта.	
		7. Составление протокола о распределении участников между экспертами для контроля за ходом выполнения задания ДЭ в соответствии с КОД 1.4 по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»	
	Работа с участниками ДЭ		
	10:00 – 11:00	1. Ответственный от образовательной организации за проведение ДЭ осуществляет контроль за подключением всех участников ДЭ к выбранному ресурсу ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие в указанное время	1. Подключение к выбранному ресурсу в указанное время
		2. Приветственное слово главного эксперта	2. Знакомство с главным экспертом
		3. Работа технического администратора площадки с участниками ДЭ по обучению работе с выбранными ресурсами: 3.1. ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие lms Moodle, системы электронного документооборота, ресурсы совместной работы (google docs и прочие) и другие (заполняется в подготовительные дни)	3. Работа с техническим администратором площадки и с ресурсами: 3.1. ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие 3.2. lms Moodle, системы электронного документооборота, ресурсы совместной работы (google docs и прочие) и другие (заполняется в подготовительные дни)
	11:00 – 11:30	1. Главный эксперт объясняет порядок регистрации	1. Прослушивают инструкцию по регистрации через выбранный

		участников демонстрационного экзамена. 2. Проверка личности с помощью сличения данных из системы и паспорта (устранение ошибок, по необходимости). 3. Главный эксперт объясняет процедуру заполнения протокола о регистрации и загрузку его на выбранный ресурс. 5.5. Проверка главным экспертом подписей в Протоколе регистрации участников ДЭ через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие	ресурс ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие
		4. Проверка личности с помощью сличения данных из системы и паспорта (устранение ошибок, по необходимости).	2. Демонстрируют с помощью веб-камеры через выбранный ресурс документов, удостоверяющих личность
		5. Главный эксперт объясняет процедуру заполнения протокола о регистрации и загрузку через выбранный ресурс ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	2.1. Заполняют Протокол о регистрации путем отметки в электронном документе, сканирования/фотографирования подписанных протоколов, электронной подписью 2.2. Загружают Протокола на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие
		6. Проверка главным экспертом подписей в Протоколе регистрации участников ДЭ через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	3. Сообщение главному эксперту о завершении загрузки подписанного протокола на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие
	11:30 – 14:00	1. Проверка главным экспертом и линейными экспертами совместно с техническим администратором площадки готовности мест участников для проведения ДЭ согласно инфраструктурного листа и	1. Подключаются в указанное время к конференции, созданной на выбранном ресурсе ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие, по очереди демонстрируют через веб-камеру или иное

		плана застройки КОД 1.4 по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» (осуществляется через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие – на каждого участника дается 5-15 минут.	видеоустройство рабочее место участника ДЭ (заранее ими подготовленное, согласно ИЛ и ПЗ указанных в КОД 1.4)
		2. Проверка ответственным линейным экспертом (можно самостоятельно или с помощью технического администратора площадки) рабочего компьютера участника ДЭ (выполняется с помощью, например, программы совместной удаленной работы TeamViewer или аналогичной)	2. Дают доступ с помощью программы teamviewer, встроенных средств систем совместной работы и ВКС
		3. Главный эксперт оформляет протокол о готовности мест участников к ДЭ	
	14:00 – 14:30	1. Проведение главным экспертом вводного инструктажа о порядке и особенностях хода ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие	1. Прослушивают инструкцию по регистрации через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие
		2. Ответы главного эксперта на вопросы участников	2. Задают вопросы главному эксперту.
	14:30 – 15:00	1. Проведение главным экспертом инструктажа участников ДЭ по охране труда и технике безопасности (осуществляется через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие	1. Прослушивание инструктажа по охране труда и технике безопасности через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие
		2. Разбор возникших вопросов от участников ДЭ	2. Разбор возникших вопросов
		3. Главный эксперт объясняет процедуру заполнения	3. Заполняют протокол об ознакомлении с ТБ и ОТ путем

		протокола об ознакомлении с ТБ и ОТ и его загрузку на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие в нужный раздел	подписания онлайн в IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие 4. Загружают на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие
		4. Проверка главным экспертом подписей в Протоколе об ознакомлении с ТБ и ОТ участников ДЭ через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	5. Сообщение главному эксперту о завершении загрузки подписанного протокола на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие
	15:00 – 16:30	1. Проведение главным экспертом жеребьевки по распределению рабочих мест, ознакомление участников с графиком работы, иной документацией (осуществляется через выбранный ресурс) с использованием программы, например, Smart Notebook, google drive (или аналог).	1. Наблюдение / участие в процессе жеребьевки в зависимости от организации процесса
		2. Знакомство с оценочными материалами и заданием его на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие ответы на вопросы от участников ДЭ	2. Знакомство с оценочными материалами и заданием на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие, вопросы главному эксперту
		3. Главный эксперт объясняет процедуру заполнения протокола о распределении рабочих мест и ознакомления участников с документацией, оборудованием и рабочими местами и его загрузку на выбранный ресурс IVA, вебинар.ру, webex, mind,	3. Заполняют протокол об ознакомлении с ТБ и ОТ путем подписания онлайн в IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие

		trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	Загружают на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие
		4. Проверка главным экспертом подписей в Протоколе о распределении рабочих мест и ознакомления участников с документацией, оборудованием и рабочими местами через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	4. Сообщение главному эксперту о завершении загрузки подписанного протокола на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие
		5. Главный эксперт объясняет процедуру заполнения протокола об ознакомлении участников демонстрационного экзамена по стандартам Ворлдскиллс Россия с оценочными материалами и заданием и его загрузку на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	5. Заполняют протокол путем подписания онлайн в IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие Загружают на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие
		6. Проверка главным экспертом подписей в Протоколе об ознакомлении участников демонстрационного экзамена по стандартам Ворлдскиллс Россия с оценочными материалами и заданием через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	6. Сообщение главному эксперту о завершении загрузки подписанного протокола на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие
		7. Знакомство линейных экспертов с закрепленными за ними участниками ДЭ	7. Знакомство с закрепленными линейными экспертами
	16:30	8. Работа главного эксперта над проверкой всех протоколов за «Подготовительный день»	8. Отключение от видео связи

День 1	08:00 – 08:30	1. Произведение техническим администратором площадки подключения связи с участниками ДЭ (осуществляется через выбранный ресурс)	1. Подключение участников ДЭ и тестирование стабильности сигнала с техническим администратором площадки (осуществляется через выбранный ресурс)
	08:30 – 09:00	1. Произведение техническим администратором площадки подключения связи с экспертами и главным экспертом ДЭ (осуществляется через выбранный ресурс)	1. Подключение участников ДЭ и тестирование стабильности сигнала с техническим администратором площадки (осуществляется через выбранный ресурс)
		2. Проведение главным экспертов и линейными экспертами проверки рабочих мест участников 3. Заполняют протокол путем подписания онлайн в IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие 4. Загружают на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	2. Участники демонстрируют рабочее место через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие и рабочий компьютер через программу (выполняется с помощью, например, программы совместной удаленной работы TeamViewer или аналогичной)
	09:00 – 09:15	1. Главный эксперт проводит инструктаж по ТБ и ОТ для участников и экспертов ДЭ. 2. Заполняют протокол подписания онлайн в IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие 3. Загружают на выбранный ресурс	1. Подписание протокола об ознакомлении с ТБ и ОТ участников ДЭ: 2. Заполняют протокол путем подписания онлайн в IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие 3. Загружают на выбранный ресурс
	09:15 – 09:30	1. Ознакомление с заданием и правилами, озвучивается главным экспертом через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие,	1. Прослушивание инструкции через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие просмотр алгоритма ЭЗ в виде документа на выбранном ресурсе IVA, вебинар.ру, webex,

		открывается в виде документа на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие
	09:40 – 10:00	1. Брифинг участников: ответы на вопросы (осуществляется через выбранный ресурс) 2. Подключение через программу совместной удаленной работы IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi или teamviewer и другие к рабочим компьютерам закрепленных участников	1. Брифинг участников: ответы на вопросы главным экспертом (осуществляется через выбранный ресурс) 2. Открытие доступа ответственным экспертам через программу совместной удаленной работы IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие
	10:00 – 13:10	1. Старт на начало выполнения задания дает главный эксперт через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие 2. Линейные эксперты наблюдают за закрепленными участниками ДЭ (с помощью программы совместной удаленной работы, через выбранный ресурс _____)	1. Участники приступают к выполнению задания согласно КОД 1.4 по компетенции «Корпоративная защита от внутренни»
	13:10 – 14:00	1. Технический администратор площадки по необходимости обеспечивает техническую поддержку 2. Главный эксперт обеспечивает контроль окончания выполнения задания	1. Загрузка участниками выполненных заданий на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие 2. Сообщение главному эксперту о завершении отправки выполненного задания
	13:10 – 14:00	1. Обеденный перерыв	
	14:00 – 17:10	3. Технический администратор площадки по необходимости обеспечивает техническую поддержку	1. Загрузка участниками выполненных заданий на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота,

		1. Главный эксперт обеспечивает контроль окончания выполнения задания	систем совместной работы и другие 2. Сообщение главному эксперту о завершении отправки выполненного задания
	16:00 – 19:10	1. Работа линейных экспертов по просмотру заданий, заполнение форм и оценочных ведомостей в Google / онлайн форм / других ресурсов 2. Технический администратор площадки обеспечивает техническую помощь экспертам по необходимости (в удаленном формате часть заданий может быть проверяться до окончания модуля) 3. Главный эксперт заносит оценки в систему CIS после получения заполненных Google / онлайн форм / других ресурсов на каждого участника	
	19:00 – 20:00	1. Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола 2. Подписание протокола о блокировки оценок 2.1. Линейные эксперты заполняют Протокол о блокировки оценок, путем подписания онлайн в IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие, 2.2. Линейные эксперты загружают протокол на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие. 2.3. Сообщение главному эксперту о завершении загрузки заполненного протокола на выбранный ресурс IVA,	

		вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	

3. Детализация инфраструктурного листа и обустройства рабочих мест участников экзамена и экспертов (ПРИМЕР)

Оснащение рабочего места участника экзамена	1. Стол 2. Стул 3. Персональный компьютер (ноутбук, моноблок или аналог) 4. Компьютерная мышь 5. Наушники с микрофоном 6. Техническое средство для записи экрана, например, OBS Studio 7. Программное обеспечение для возможности удаленного подключения к компьютеру (например, TeamViewer) 8. Виртуальный диск (облако), привязанный к электронной почте. Выбор ресурса осуществляется в подготовительные дни. 9. Программа подключения к системе видеосвязи (обычно в браузере или в скачиваемом клиенте) 10. Программное обеспечение 10.1. OBS Studio 10.2. VPN клиент (при необходимости) 10.3. RDP/VNC/прочий клиент (при необходимости) 11. Интернет (скорость передачи данных не менее 5 Mbit/s (рекомендуемое 50 Mbit/s)) 12. Канцелярские товары (ручка, карандаш, ножницы, бумага А4) 13. Размер "Зоны демонстрации" не менее 1,5м*1,5м 14. Доступ к онлайн ресурсам совместной работы (выбирается в подготовительные дни) 14.1. IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие 15. Лампа при недостаточном освещении лица / невозможности идентифицировать документ 16. Мобильное устройство с камерой для «сканирования» документов при необходимости. Необходимость уточняется в подготовительные дни.
Оснащение рабочего места главного эксперта	1. Стол 2. Стул 3. Персональный компьютер (ноутбук, моноблок или аналог) 4. Наушники с микрофоном

	5. Интернет (скорость передачи данных не менее 15 Mbit/s (рекомендуемое 100 Mbit/s)) 6. Программное обеспечение и его функции. 6.1. Клиент подключения к системе видеосвязи (обычно браузер) 6.2. VPN клиент (при необходимости) 6.3. RDP/VNC/прочий клиент (при необходимости) 7. МФУ или принтер + приложение-сканер для мобильного устройства с помощью камеры 8. Канцелярские товары (ручка, карандаш, линейка, степлер, скобы, ножницы, скотч, Бумага А4, файлы, папка скоросшиватель) 9. Доступ к онлайн ресурсам совместной работы (выбирается в подготовительные дни) 9.1. . 9.2. .
Оснащение рабочих мест членов экспертной группы	1. Стол 2. Стул 3. Персональный компьютер (ноутбук, моноблок или аналог) – по количеству участников ДЭ 4. Наушники с микрофоном 5. Интернет или Wi-fi (скорость передачи данных не менее 5 Mb (рекомендуемое 100 Mb)) 6. Программное обеспечение и его функции 9.3. Клиент подключения к системе видеосвязи (обычно браузер) 6.1. VPN клиент (при необходимости) 6.2. RDP/VNC/прочий клиент (при необходимости) 7. Доступ к онлайн ресурсам совместной работы (выбирается в подготовительные дни) 7.1. . 7.2. . 8. Канцелярские товары (ручка, карандаш, ножницы, бумага А4)

4. Условия работы экспертной группы (ПРИМЕР)

1. Эксперты закрепляются за участниками (не более 4 участников на одного линейного эксперта) с целью контроля выполнения задания (осуществляется через ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, систем совместной работы и другие) (выбирается в подготовительные дни).
2. Просмотр демонстрируемых участником заданий через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы удаленного контроля систем совместной работы и другие (выбирается в подготовительные дни).

3. Оценка работ участников через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие (выбирается в подготовительные дни).
4. В зависимости от количества участников демонстрационного экзамена может увеличиваться время на просмотр и оценку работ участников.
5. Информация по ЭЗ в виде документа расположена на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие (выбирается в подготовительные дни), доступ к которой осуществляется главным экспертом.

5. Дополнительные условия (ПРИМЕР)

5.1. Требования к отбору линейных экспертов:

1. Наличие устойчивого интернета на месте проведения оценки. Не допускается работа экспертов в движении (например, из поезда, автомобиля, прочего транспорта). Не рекомендуется работать в шумных местах (учебный класс, кафе, прочее).
2. Свободное пользование ПК и возможность установки программного обеспечения по запросу ГЭ/ТЭ
3. Наличие требований согласно WSR

5.2. Деятельность в рамках ДЭ (ПРИМЕР)

Наименование деятельности	Дни				
	С-3	С-2	С-1	С1	С2
5.2.1. Обязанности главного эксперта					
1. Работа по подготовке рабочих мест линейных экспертов и участников, согласно инфраструктурного листа КОД 1.4 по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» с техническим администратором площадки и ответственным от образовательной организации за проведение ДЭ	×	×	×		
2. Подготовка и передача контент-папки в соответствии с КОД 1.4 по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» для загрузки на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие техническому администратору площадку		×	×		
3. Предоставление техническому администратору площадки материалы для загрузки на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие: 3.1. инструкция по ТБ и ОТ, 3.2. план застройки площадки, 3.3. SMP, 3.4. техническое описание компетенции, 3.5. инфраструктурный лист согласно КОД 1.4 3.6. образец КОД по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» 3.7. кодекс этики.	×	×			
4. Создание Google / онлайн форм / других ресурсов для проведения оценочной деятельности по КОД 1.4 по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»	×	×	×		
5. Проверка данных в системе CIS			×		
6. Подготовка протоколов (на все дни ДЭ) и сигнальных карточек: 6.1. протоколы для экспертов 6.2. протоколы для участников			×		
7. Подготовка протокола о готовности мест экспертов и участников к ДЭ в соответствии с КОД 1.4 компетенции «Корпоративная защита от внутренних угроз информационной безопасности»			×		
8. Организация работы совместно с техническим администратором площадки линейных экспертов			×		
9. Регистрация главным экспертом линейных экспертов ДЭ (осуществляется через выбранный ресурс)			×	×	

Наименование деятельности	Дни				
	С-3	С-2	С-1	С1	С2
10. Регистрация главным экспертом участников ДЭ (осуществляется через выбранный ресурс)			×	×	
11. Проведение главным экспертом инструктажа по ТБ и ОТ с линейными экспертами (осуществляется через выбранный ресурс)			×	×	
12. Проведение главным экспертом инструктажа по ТБ и ОТ с участниками ДЭ (осуществляется через выбранный ресурс)			×	×	
13. Предоставление техническому администратору площадки материалы по заданию для загрузки на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие			×	×	
14. Распределение главным экспертом обязанностей по проведению ДЭ между членами Экспертной группы (осуществляется через выбранный ресурс), заполнение Протокола о распределении судейских ролей в Google / онлайн форм / других ресурсов форме			×		
15. Распределение главным экспертом между экспертами участников для наблюдения за выполнением экзаменационного задания с помощью программы IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие (осуществляется через выбранный ресурс)			×	×	
16. Ознакомление участников ДЭ с заданием в соответствии с КОД 1.4 компетенции «Корпоративная защита от внутренних угроз информационной безопасности»			×	×	
17. Проведение жеребьевки по распределению рабочих мест участников ДЭ (осуществляется через выбранный ресурс, с помощью программы IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие)			×		
18. Ознакомление участников с документацией, оборудованием и рабочими местами (осуществляется через выбранный ресурс, на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие)			×	×	
19. 19. Ознакомление участников ДЭ с санкциями при несоблюдении правил проведения ДЭ			×		
20. Ознакомление участников с 30% изменения по заданию в соответствии с КОД 1.4 компетенции «Корпоративная защита от внутренних угроз информационной безопасности» (через выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие)			×	×	

Наименование деятельности	Дни				
	С-3	С-2	С-1	С1	С2
21. Сбор протоколов в день С-1: **21.1. «Протоколы экспертов день С-1»** 21.2. Протокол регистрации экспертов, 21.3. Протокол ТБ и ОТ экспертов, 21.4. Протокол распределения судейских ролей, 21.5. Протокол о готовности рабочих мест участников ДЭ, 21.6. Протокол блокировки критериев оценки. **21.7. «Протоколы участников ДЭ С-1»** 21.8. Протокол регистрации участников 21.9. Протокол ТБ и ОТ участников 21.10. Протокол распределения рабочих мест и ознакомления участников с документацией, оборудованием и рабочими местами 21.11. Протокол об ознакомлении участников демонстрационного экзамена по стандартам Ворлдскиллс Россия с оценочными материалами и заданием			×		
22. Сбор протоколов в день С1: **22.1. «Протоколы экспертов день С1»** 22.2. Протокол ТБ и ОТ экспертов 22.3. Протокол о готовности рабочих мест участников ДЭ 22.4. Протокол учета времени 22.5. Итоговый протокол блокировки **22.6. «Протоколы участников ДЭ С1»** 22.7. Протокол ТБ и ОТ участников			×		
23. Занесение оценок в систему CIS				×	
24. Организация сверки внесенных оценок ответственным от образовательной организации за проведение ДЭ				×	
25. Блокировка критериев оценки				×	
26. Подготовка отчета по итогу проведения ДЭ в соответствии с КОД 1.4 компетенции «Корпоративная защита от внутренних угроз информационной безопасности»				×	×
5.2.2.Обязанности Технического администратора площадки					
1. Создание ветки на выбранном ресурсе _____ (рекомендуется LMS Moodle или аналогичное) для проведения ДЭ, необходимые разделы: 1.1. **раздел 1. «Нормативные документы»** включает следующие документы: инструкция по ТБ и ОТ, план застройки площадки, SMP, Техническое описание компетенции, инфраструктурный лист согласно КОД 1.4, методика проведения ДЭ, образец КОД по компетенции «Корпоративная защита от внутренних угроз информационной безопасности», кодекс этики; 1.2. **раздел 2. «Задание ДЭ в соответствии с КОД 1.4 по компетенции** «Корпоративная защита от внутренних угроз информационной безопасности»: загружается главным экспертом в день С-1; **1.3. раздел 3. «Работы экзаменуемых»**	×	×	×	×	

Наименование деятельности	Дни				
	С-3	С-2	С-1	С1	С2
1.4. раздел 4. «Протоколы экспертов день С-1» 1.4.1. Ответ на задание № 1 «Протокол регистрации экспертов» 1.4.2. Ответ на задание № 2 «Протокол ТБ и ОТ экспертов» 1.4.3. Ответ на задание № 3 «Протокол распределения судейских ролей» 1.4.4. Ответ на задание № 4 «Протокол о готовности рабочих мест участников ДЭ» **1.5. раздел 5. «Протоколы участников ДЭ С-1»** 1.5.1. Ответ на задание № 1 «Протокол регистрации участников» 1.5.2. Ответ на задание № 2 «Протокол ТБ и ОТ участников» 1.5.3. Ответ на задание № 3 «Протокол распределения рабочих мест и ознакомления участников с документацией, оборудованием и рабочими местами» 1.5.4. Ответ на задание № 4 «Протокол об ознакомлении участников демонстрационного экзамена по стандартам Ворлдскиллс Россия с оценочными материалами и заданием» **1.6. раздел 6. «Протоколы экспертов день С1»** 1.6.1. Ответ на задание № 1 «Протокол ТБ и ОТ экспертов» 1.6.2. Ответ на задание № 2 «Протокол о готовности рабочих мест участников ДЭ» 1.6.3. Ответ на задание № 3 «Протокол учета времени» **1.7. раздел 7. «Протоколы участников ДЭ С1»** 1.7.1. Ответ на задание № 1 «Протокол ТБ и ОТ участников» 1.7.2. Ответ на задание № 2 «Протокол распределения рабочих мест и ознакомления участников с документацией, оборудованием и рабочими местами»					
2. Загрузка документов, присланных главным экспертом в указанные разделы на выбранный ресурс IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие	×	×	×	×	
3. Создание личных кабинетов: главному эксперту, участникам и линейным экспертам ДЭ.	×	×	×		
4. Предоставление доступа к личному кабинету: главному эксперту, участникам и линейным экспертам ДЭ (осуществляется путем рассылки на e-mail предоставленные ответственным от образовательной организации за проведение ДЭ)	×	×	×		
5. Оснащение рабочих мест участников, линейных экспертов согласно инфраструктурному листу КОД 1.4 по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»	×	×	×		
6. Подготовка печатного пакета протоколов (на все дни ДЭ) и сигнальных карточек персонально для каждого участника и		×	×		

Наименование деятельности	Дни				
	С-3	С-2	С-1	С1	С2
линейного эксперта по ДЭ (присылается главным экспертом)					
7. 7. Проверка и дополнительная настройка/установка (по необходимости) программного обеспечения рабочих компьютеров участников ДЭ	×	×	×		
8. Проверка и дополнительная настройка/установка (по необходимости) программного обеспечения рабочих компьютеров главного эксперта и линейных экспертов	×	×	×		
9. Обучение работе с программным обеспечением главного эксперта и линейных экспертов ДЭ		×	×		
10. Обучение работе с программным обеспечением участников ДЭ			×		
11. Обучение работе на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие (рекомендуется LMS Moodle совместно с ВКС или аналогичное): 11.1. линейным экспертам (вход, скачивание работ участников ДЭ); 11.2. главный эксперт (вход, загрузка документов, настройка времени и количества возможного погружения файлов (один раз, один файл), скрытие документов до момента официального начала ДЭ, открытие документа, скачивание документов участников для проверки задания ДЭ).	×	×	×		
12. Обучение работе на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие (рекомендуется LMS Moodle совместно с ВКС или аналогичное) (рекомендуется LMS Moodle или аналогичное) участников (вход, скачивание документов, загрузка документов, проверка загруженного документа).		×	×		
13. Обучение работы на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие (рекомендуется LMS Moodle совместно с ВКС или аналогичное) (рекомендуется LMS Moodle или аналогичное) главного эксперта и линейных экспертов ДЭ	×	×	×		
14. Обучение работы на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие (рекомендуется LMS Moodle совместно с ВКС или аналогичное) (рекомендуется LMS Moodle или аналогичное) участников ДЭ		×	×		
15. Проверка совместно с главным экспертом готовности рабочих мест участников и линейных экспертов к ДЭ в соответствии с КОД 1.4 по компетенции «Корпоративная		×	×		

Наименование деятельности	Дни				
	С-3	С-2	С-1	С1	С2
защита от внутренних угроз информационной безопасности» согласно SMP					
16. Обеспечение технической поддержки по необходимости			×	×	
17. Сбор предоставленного оборудования (если применимо)					
18. Осуществление сбора, хранения и размещения видеозаписей процедуры подготовки и проведения ДЭ			×	×	×
5.2.3. Обязанности ответственного от образовательной организации за проведение ДЭ					
1. Предоставление информации главному эксперту: 1.1. даты ДЭ и № КОД выбранный образовательной организацией, контакты технического администратора площадки и ответственного от образовательной организации за проведение ДЭ (указание ФИО, email, телефон); 1.2. скан аттестата об аккредитации ЦПДЭ в соответствии с КОД; 1.3. список участников (ФИО) в формате Excel; 1.4. список линейных экспертов (указание ФИО, места работы, должность, номер свидетельства и срок действия, email, телефон) в формате Excel	×	×	×		
2. Проверка e-mail: главного эксперта, участников и линейных экспертов ДЭ		×	×		
3. Предоставление информации техническому администратору площадки и главному эксперту (осуществляется через e-mail)	×	×	×		
4. Передача пакета печатных протоколов (на все дни ДЭ) и сигнальных карточек персонально для каждого участника и линейного эксперта по ДЭ	×	×	×		
5. Обеспечение совместно с техническим администратором площадки застройки рабочих мест участников и линейных экспертов ДЭ согласно инфраструктурному листу КОД 1.4 по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»	×	×	×		
6. Контроль явки и выполнения работ в установленное время (согласно SMP) участников, линейных экспертов ДЭ и технического администратора площадки			×	×	
7. Сверка внесенных оценок ответственным от образовательной организации за проведение ДЭ				×	
8. Сбор предоставленного оборудования (если применимо)					
5.2.4.Обязанности линейных экспертов					
1. Ознакомление с нормативной документацией и правилами проведения ДЭ (осуществляется через выбранный ресурс, на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие)		×	×		
2. Ознакомление с работой:			×	×	

Наименование деятельности	Дни				
	С-3	С-2	С-1	С1	С2
2.1. на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие 2.2. на Google / онлайн форм / других ресурсов, 2.3. с программой удаленного доступа / удаленной совместной работы.					
3. Заполнение протоколов в день С-1: 3.1. Протокол регистрации экспертов, 3.2. Протокол ТБ и ОТ экспертов, 3.3. Протокол распределения судейских ролей, 3.4. Протокол о готовности рабочих мест участников ДЭ.			×		
4. Проверка готовности рабочего места закрепленных участников ДЭ в соответствии с жеребьевкой.			×	×	
5. Заполнение протоколов день С1: 5.1. Протокол регистрации экспертов 5.2. Протокол ТБ и ОТ экспертов 5.3. Протокол о готовности рабочих мест участников ДЭ 5.4. Протокол учета времени				×	
6. Наблюдение за соблюдением правил проведения ДЭ и ТБ и ОТ участниками при выполнении задания.				×	
7. Осуществление оценки выполненного задания ДЭ участниками в соответствии с КОД 1.4 компетенции «Корпоративная защита от внутренних угроз информационной безопасности» и заполнение ведомостей				×	
8. Подписание итогового отчета проведения ДЭ через Google / онлайн форм / других ресурсов				×	×
9. В случае ухудшения обзора за участником при выполнении задания ДЭ попросить участника повернуть/направить камеру в сторону выполнения видеосъемки производственной гимнастики				×	
5.2.5.Обязанности участников, сдающих ДЭ по компетенции					
1. Ознакомление с нормативной документацией и правилами проведения ДЭ (осуществляется через выбранный ресурс, на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi, системы электронного документооборота, систем совместной работы и другие)		×	×		
2. Ознакомление с работой: 2.1. на выбранном ресурсе IVA, вебинар.ру, webex, mind, trueconf, zoom, skype, jitsi и другие 2.2. на Google / онлайн форм / других ресурсов, 2.3. с программой удаленного доступа / удаленной совместной работы.		×	×		
3. Заполнение протоколов в день С-1: 3.1. Протокол регистрации участников 3.2. Протокол ТБ и ОТ участников			×		

Наименование деятельности	Дни				
	С-3	С-2	С-1	С1	С2
3.3. Протокол распределения рабочих мест и ознакомления участников с документацией, оборудованием и рабочими местами 3.4. Протокол об ознакомлении участников демонстрационного экзамена по стандартам Ворлдскиллс Россия с оценочными материалами и заданием					
4. Заполнение протоколов в день С1: 4.1. Протокол регистрации участников 4.2. Протокол ТБ и ОТ участников 4.3. Протокол распределения рабочих мест и ознакомления участников с документацией, оборудованием и рабочими местами 4.4. Протокол об ознакомлении участников демонстрационного экзамена по стандартам Ворлдскиллс Россия с оценочными материалами и заданием				×	
5. Ознакомление с заданием ДЭ в соответствии с КОД 1.4 компетенции «Корпоративная защита от внутренних угроз информационной безопасности» и заполнении ведомости			×	×	
6. Ознакомление с 30 % изменений в соответствии с КОД 1.4 компетенции «Корпоративная защита от внутренних угроз информационной безопасности» и заполнении ведомости			×	×	
7. Ознакомление с санкциями при несоблюдении правил проведения ДЭ			×	×	
8. Ознакомление с контент-папкой в соответствии с КОД 1.4 компетенции «Корпоративная защита от внутренних угроз информационной безопасности»		×	×	×	
9. Выполнение задания в соответствии с КОД 1.4 компетенции «Корпоративная защита от внутренних угроз информационной безопасности» и правилами проведения ДЭ				×	
10. Применение сигнальных карточек в случае необходимости с оповещением закрепленного за участником ДЭ линейного эксперта				×	
11. В случае окончания выполнения задания раньше отведенного времени сообщить об этом закрепленному за ним линейному эксперту				×	

5.3. Правила проведения ДЭ для участников: (ПРИМЕР)

1. Допустимо использование смартфонов, только для осуществления видеосъемки и идентификации в случае отсутствия веб-камеры на ПК.

2. Место нахождения смартфона должно быть в зоне видимости ответственного линейного эксперта / главного эксперта.

3. В случае обнаружения использования смартфона, с целью домашней заготовки видеофрагмента, использования не разрешенной информации из интернета, звонка, использования мессенджеров обнулить критерии по оценке работы участника.

Комплект оценочной документации № 2.1 для Демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

СОДЕРЖАНИЕ

Паспорт комплекта оценочной документации (КОД) № 2.1 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Комплект оценочной документации (КОД) № 2.1 разработан в целях организации и проведения демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» и рассчитан на выполнение заданий продолжительностью 12 часов.

КОД № 2.1 может быть рекомендован для оценки освоения основных профессиональных образовательных программ и их частей, дополнительных профессиональных программ и программ профессионального обучения, а также на соответствие уровням квалификации согласно Таблице (Приложение).

1. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации № 2.1 (Таблица 1).

Таблица 1.

Раздел WSSS	Наименование раздела WSSS	Важность (%)
1	**Организация работы и управление**	**3**
2	**Установка, конфигурирование и устранение неисправностей**	**20,3**
4	**Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**	**20,8**
5	**Технологии анализа и защиты сетевого трафика**	**19,7**
6	**Технологии агентского мониторинга**	**13**
7	**Анализ выявленных инцидентов. Подготовка отчетов, классификация угроз и инцидентов**	**2,2**

Таблица 2.

Раздел WSSS	Наименование раздела WSSS
1.	Организация работы и управление
	Специалист должен знать и понимать: • Понимание принципов работы специалиста по информационной безопасности и их применение;

	• Знание принципов и положений безопасной работы в общем и по отношению к корпоративной среде; • Регламентирующие документы в области безопасности информационных систем; • Регламентирующие документы в области охраны труда и безопасности жизнедеятельности; • Важность организации труда в соответствии с методиками; • Методы и технологии исследования; • Важность управления собственным профессиональным развитием; • Скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню. • Важность умения слушать собеседника как части эффективной коммуникации; • Роли и требования коллег, и наиболее эффективные методы коммуникации; • Важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими; • Способы разрешения непонимания и конфликтующих требований; • Методы управления стрессом и гневом для разрешения сложных ситуаций.
	Специалист должен уметь: • Поддерживать безопасную, аккуратную и эффективную рабочую зону; • Использовать все оборудование и программное обеспечение безопасно и в соответствии с инструкциями производителя; • Следовать предписаниям в области охраны труда и безопасности жизнедеятельности; • Регулярно планировать свою работу и корректировать планы в соответствии с изменяющимися приоритетами; • Поддерживать рабочее место в должном состоянии и порядке. • Демонстрировать развитые способности слушать и задавать вопросы для более глубокого понимания сложных ситуаций; • Выстраивать эффективное письменное и устное общение; • Понимать изменяющиеся требования и адаптироваться к ним;
2.	Установка, конфигурирование и устранение неисправностей
	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 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 Windows Server и Linux Red Hat Enterprise Linux; • 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;
4.	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз
	Специалист должен знать и понимать: • Технологии работы с политиками информационной безопасности; • Создание новых политик, модификация существующих; • Общие принципы при работе интерфейсом системы защиты корпоративной информации; • Объекты защиты, персоны; • Ключевые технологии анализа трафика; • Типовые протоколы и потоки данных в корпоративной среде, такими как: • корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4) • веб-почта; • Интернет-ресурсы: сайты, блоги, форумы и т. д. (протоколы HTTP, HTTPS); • социальные сети; • интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP; • принтеры: печать файлов на локальных и сетевых принтерах; • любые съемные носители и устройства; • Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек; • Типы угроз информационной безопасности, типы инцидентов, • Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации; • Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации; • Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных; • Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации; • Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки; • Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе; • Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов; • Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации;
	Специалист должен уметь: • Создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты; • Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; • Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии;

	• Работа со сводками, виджетами, сводками; • Работа с персонами; • Работа с объектами защиты; • Провести имитацию процесса утечки конфиденциальной информации в системе; • Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; • Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. • Работа с категориями и терминами; • Использование регулярных выражений; • Использование морфологического поиска; • Работа с графическими объектами; • Работа с выгрузками и баз данных; • Работа с печатями и бланками; • Работа с файловыми типами; • Эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;
5.	**Технологии анализа и защиты сетевого трафика**
	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 • Технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений; • Ключевые компоненты VPN-сетей; • Особенности VPN-сети и механизмы их управления; • Современные криптографические алгоритмы. Криптопровайдеры, криптографические интерфейсы и библиотеки; • Архитектура, основные компоненты PKI их функции и взаимодействие; • Жизненный цикл ключей и сертификатов; • Электронный сертификат ключей ЭЦП. 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; • 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;
6.	Технологии агентского мониторинга
	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.
	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.
7.	Анализ выявленных инцидентов. Подготовка отчетов, классификация угроз и инцидентов
	Специалист должен знать и понимать: • Основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах; • Инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз; • Типовой пакет нормативных документов, необходимого для развёртывания и эксплуатации системы корпоративной защиты в организации;

	• Виды типовых отчетных форм о выявленных угрозах и инцидентах; • Типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации; • Понимать подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз; • Системы DLP и требования по информационной безопасности. • Категорирование информации в РФ. • Юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; Специальные технические средства • Меры по обеспечению юридической значимости DLP (Pre-DLP). Практику право применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (Post-DLP).
	Специалист должен уметь: • Разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности; • Проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации; • Создавать отчёты о выявленных инцидентах, угрозах и т.п. Представлять отчёты руководству, обосновывать полученные результаты анализа.

2. Формат Демонстрационного экзамена:

Очный

3. Форма участия:

Индивидуальная

4. Вид аттестации:

ГИА

5. Обобщенная оценочная ведомость.

В данном разделе определяются критерии оценки и количество начисляемых баллов (судейские и объективные) (Таблица 3).

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 79.

Таблица 3.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
1.	1. Установка и конфигурирование компонентов DLP системы	A. Организация работы и управление B. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	2 часа	1, 2	0	18	18
2.	2. Технологии агентского мониторинга	C. Технологии агентского мониторинга	1,5 часа	6	0	13	13
3.	3. Разработка и применение политик, анализ выявленных инцидентов	D. Разработка политик безопасности, анализ выявленных инцидентов	3 часа	4, 7	0	23	23
4.	4. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	E. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	2,5 часа	2, 5	0	12,3	12,3
5.	5. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	F. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	3 часа	5, 2.	0	12,7	12,7
				Итого		79	79

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

6.1. Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности» — 3 чел.

6.2. Расчет количества экспертов исходя из количества рабочих мест и участников осуществляется по схеме согласно Таблице 4:

Таблица 4.

Количество постов-рабочих мест / Количество участников	1-4	5-8	9-12	13-16	17-20	21-25
От 1 до 5	3	3				
От 6 до 10		3	3			
От 11 до 15			4	4		
От 16 до 20				5	5	
От 21 до 25						6

7. Список оборудования и материалов, запрещенных на площадке

– Мобильные телефоны, смартфоны, рации, беспроводные, проводные наушники и другие средства связи;

– Собственные заметки, шпаргалки, книги и прочие документы;

– Личная электронная почта, мессенджеры и прочие средства связи посредством сети Интернет за исключение разрешенных ресурсов для тестирования систем в процессе работы;

– Компьютеры, ноутбуки, планшеты и прочие устройства, за исключением устройств, предоставленных площадкой;

– Периферийные устройства (клавиатуры, манипуляторы типа мышь и прочие устройства) за исключением устройств, предоставленных площадкой.

Задание для демонстрационного экзамена по комплекту оценочной документации № 2.1 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

(образец)

Задание включает в себя следующие разделы:

1. Формат Демонстрационного экзамена
2. Формы участия
3. Вид аттестации
4. Модули задания, критерии оценки и необходимое время
5. Необходимые приложения

Продолжительность выполнения задания: 12 ч.

1. Формат Демонстрационного экзамена:

Очный

2. Форма участия:

Индивидуальная

3. Вид аттестации:

ГИА

4. Модули задания, критерии оценки и необходимое время

Модули и время сведены в Таблице 1.

Таблица 1.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
6.	1. Установка и конфигурирование компонентов DLP системы	A. Организация работы и управление B. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	2 часа	1, 2	0	18	18
7.	2. Технологии агентского мониторинга	C. Технологии агентского мониторинга	1,5 часа	6	0	13	13
8.	3. Разработка и применение политик, анализ выявленных инцидентов	D. Разработка политик безопасности, анализ выявленных инцидентов	3 часа	4, 7	0	23	23
9.	4. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	E. Технологии анализа и защиты сетевого трафика, установка и конфигурирование	2,5 часа	2, 5	0	12,3	12,3
10.	5. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	F. Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование	3 часа	5, 2	0	12,7	12,7
				Итого		79	79

Модули с описанием работ

Модуль 1: Установка и конфигурирование компонентов DLP системы

Введение

В компания «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 носители информации, электронная почта и различные интернет-ресурсы.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены, но IP адреса нужно назначить согласно прилагаемой карточке. Подготовлены следующие виртуальные машины для дальнейшей работы:

- AD Сервер с контроллером домена
- DLP сервер установлен (но не настроен), активирована лицензия
- Виртуальная машина для установки сервера агентского мониторинга
- Виртуальные машины «нарушителей» для установки агентов

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов. До установки системы необходимо подготовить доменных пользователей в соответствии с заданием.

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 номером рабочего места (например, server-16).

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

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например: Задание_5_копирование.jpg.

Задание 1: Настройка контроллера домена

Необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: user1, пароль: 12345678, запретить локальный вход в систему

Логин: user2, пароль: 12345678, запретить локальный вход в систему

Логин: user3, пароль: 12345678, права администратора домена и локального администратора

Логин: user4, пароль 12345678, права пользователя домена

Задание 2: Настройка DLP сервера

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

Необходимо вычислить IP-адрес сервера через локальную консоль виртуальной машины.

Настроить DNS на сервере для корректной работы.

Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам.

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

Для входа в веб-консоль необходимо использовать ранее созданного пользователя домена с полными правами 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» с заголовком IWTM.

Корректно выполненным заданием будет являться работоспособная система с верно настроенными параметрами.

Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить базу данных с паролем суперпользователя 12345678.

Установить сервер агентского мониторинга с параметрами по умолчанию.

При установке необходимо установить соединение с DLP-сервером контроля сетевого трафика по IP-адресу и токену, но можно сделать это и после установки сервера агентского мониторинга.

Настроить пользователя консоли управления: officer с паролем 12345678.

Синхронизировать каталог пользователей и компьютеров с Active Directory.

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

Зафиксировать факт создания пользователя и настройку скриншотом.

Проверить работоспособность входа в консоль управления без ввода пароля. Стоит обратить внимание, что если сервер не введен в домен, данная опция работать не будет.

Зафиксировать факт подключения без пароля скриншотом.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» с заголовком IWDM.

Задание 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить агент мониторинга с помощью задачи первичного распространения с сервера агентского мониторинга. Необходимо учесть, что установка осуществляется только с правами администратора (доменного или локального). Ручная установка с помощью создания пакета установки является неверным выполнением задания.

Зафиксировать успешное выполнение задачи скриншотом

В случае проблем стоит проверить настройки брандмауэра и DNS.

Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)

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

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

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога.

Зафиксировать выполнение задания скриншотом настройки в web-консоли.

Стоит учесть, что неправильная настройка DNS на серверных машинах, а также неправильные настройки брандмауэра могут привести к неработоспособной системе сканирования сетевых ресурсов.

Задание 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания событий) для данных, содержащих слово «Экзамен», установить низкий уровень угрозы для всех событий, добавить тег «Экзамен».

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

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена).

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задание 7: Защита системы с помощью сертификатов

Создайте цифровой сертификат (дерево сертификатов) формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности, длине ключа 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)
- сертификат сервиса (веб-сайта)
- Итоговый результат должен включать:
- Дерево из 2 (3)-х сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов.
- Содержимое команд по генерации ключей и сертификатов в текстовом файле «отчет.txt»
- Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе просмотра сертификатов Windows (закладки «Общие», «Путь сертифкации»).

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

Генерацию сертификатов зафиксируйте скриншотами.

Модуль 2: Технологии агентского мониторинга

Задания выполняются только с помощью компонентов DLP системы (не групповыми политиками или аналогичными решениями).

Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т.д. в соответствии с заданием, например, «Политика 1» или «Правило 1.2» и т.д.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 2».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CP-1.jpg

где CP – сокращение от англ. creating a policy, 1 – номер задания

Пример 2 для сохранения скриншота работающей политики: PW-1.jpg

где PW – сокращение от англ. policy work, 1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики:

PW-1-2.jpg

где PW – сокращение от англ. policy work, 1 – номер задания; 2 – номер скриншота для задания 1.

Задание 1

Необходимо создать новую политику, применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику.

Зафиксировать выполнение скриншотом.

Задание 2

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

Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли с указанием адреса.

Задание 3

Для удаленного управления необходимо создать дополнительного локального офицера безопасности для доступа к серверу агентского мониторинга с полными правами на управление и просмотр разделов.

Имя пользователя: user1, пароль: 12345678

Проверить работоспособность с удаленной консоли, установленной ранее, зафиксировать выполнение скриншотом.

Задание 4

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 5

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 6

Необходимо поставить на контроль буфер обмена в текстовых процессорах.

Проверить работоспособность и зафиксировать выполнение занесением пары событий в веб-консоль DLP-сервера на любые политики. Также подтвердить выполнение скриншотом.

Задание 7

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Задание 8

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 9

С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе.

Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.

Задание 10

Создать политику по блокировке копирования файлов формата zip на USB-накопители.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 11

Необходимо поставить на контроль печать документов на принтерах. Продемонстрировать работоспособность на любую из политик.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 12

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 15 секунд или при переходе на другую страницу.

Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в веб-консоли DLP-сервера. Подтвердить выполнение задания скриншотами.

Задание 13

Заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 14

Осуществить выдачу временного доступа (30 минут) клиенту до заблокированного CD привода.

Зафиксировать скриншотами факт выдачи доступа и необходимые действия для выдачи доступа.

Задание 15

На машине нарушителя необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 16

Необходимо установить (сменить) пароль для удаления агента мониторинга на машине нарушителя с помощью средств сервера агентского мониторинга (удаленно).

Проверить работоспособность и зафиксировать выполнение скриншотом

Модуль 3: Разработка и применение политик, анализ выявленных инцидентов

Введение

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Для некоторых политик необходима работа с разными разделами консоли управления: категориями и терминами, технологиями, объектами защиты и т. п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, необходимо самостоятельно задать уровень угрозы).

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации с AD-сервером компании

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, т. к. легальные события не должны маркироваться как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Проверьте синхронизацию времени на всех системах, т. к. расхождение во времени между системами может повлиять на актуальность событий.

Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти в папке «Additional files» в общей папке из дополнительных сведений.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 3».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: 01-CP.jpg, де CP – сокращение от англ. creating a policy, 01 – номер задания

Пример 2 для сохранения скриншота работающей политики: 04-PW-1.jpg, 04-PW-2.jpg, где PW – сокращение от англ. policy work, 04 – номер задания, 1,2 – номер скриншотов

Задания на разработку политик можно выполнять в любом порядке.

ВНИМАНИЕ!

Необходимо называть политики / объекты / категории / теги и прочее ТОЛЬКО в соответствии с номером и названием задания

Политики — Политика X, например, «Политика 4».

Для комбинированных политик формат: Политика 4.1, 4.2 и т.д.

Объект защиты — Объект X, например, «Объект 11».

ВНИМАНИЕ!

Все политики «по умолчанию», находящиеся в консоли управления в процессе выполнения заданий должны быть отключены или удалены, так как могут помешать корректной оценке.

ВНИМАНИЕ!

При разработке и тестировании политик стоит учитывать, что нарушителем могут являться не только указанные в задании пользователи, а еще и виртуальная машина с агентом мониторинга.

ВНИМАНИЕ!

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.

Задание 1

Создайте локальную группу пользователей «Сотрудники под наблюдением». Добавьте в нее трех любых пользователей. Подтвердите выполнение задания скриншотами.

Задание 2

Для работы системы необходимо настроить периметр компании:

Почтовый домен: demo.lab.

Список веб ресурсов необходимо создать и назвать «Доверенные домены»: worldskills.org, filialdemo.lab, demolab-info.ru, dlpsystems.lab.

Группа персон 1: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Задание 3

Для недавно нанятого аудитора компании необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей без возможности редактирования. Области видимости: все.

Логин: auditor, пароль: 12345678
Подтвердите выполнение задания скриншотами.

Политика 4

В связи с секретностью при организации очередного WorldSkills, совет директоров решил контролировать передачу информации о WorldSkills за

пределы компании. В связи с этим необходимо создать политику на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills».

Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять пробел между словами, например: «Ворлд Skills». Ложных срабатываний быть не должно (например, просто на Ворлд или Skills).

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: мобильники

Проверить работоспособность.

Политика 5

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%.

Для пустого документа:

Вердикт: разрешить √

Уровень нарушения: нет

Тег: договор

Для заполненного документа:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: договор

Проверить работоспособность.

Политика 6

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании, запрещая любую внешнюю передачу документов,

содержащих заполненные бланках, при этом пустые бланки контролировать не нужно.

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 7

Для мониторинга движения официальных документов необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Политика 8

В компании происходит передача сообщений, содержащих специальные коды доступа к внутренней информационной системе. Все коды находятся в документе «Коды компании» (10 штук). Необходимо контролировать коды внутри компании, но запрещать передачу за пределы.

Передача кодов внутри компании:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: коды

Передача кодов за пределы компании:

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 9

Ракетное вооружение для авиационных комплексов различного класса, в разработке которого участвует компания, планируется к внедрению в эксплуатацию. Информация о технике может иметь конфиденциальный и секретный характер, хотя и не содержать гриф.

Необходимо блокировать любые попытки передачи данных об этих объектах на внешние адреса. Технические объекты задаются буквенно-цифирными кодами на русском языке:

Р-Цифры-Буквы или РЦифрыБуква или Р-ЦифрыБуква

- Р – русская буква «Р»
- Цифры – не более 4-х подряд, например, 27 или 5000 (обязательно наличие хотя бы одной цифры)
- Буквы – от 1 до 2-х подряд, например, Р-27АЭ

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: ракеты

Проверить работоспособность.

Политика 10

Сотрудники отдела ИТ 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 отдела информатизации.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: база

Проверить работоспособность.

Политика 11

В связи с постоянными заказами на транспортировку больших грузов, сотрудники компании подрабатывают в тайне от начальства, занимаясь попутной перевозкой других грузов, а также пассажиров. В связи с этим необходимо отслеживать в почтовых сообщениях упоминания об автостопе, халтуре, подработке, грузовом такси.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: подработка

Проверить работоспособность.

Политика 12

Необходимо запретить передачу документов с грифом (информационной меткой) «ООО Demo Lab. Конфиденциально» или «ООО Demo Lab. Строго конфиденциально» любым сотрудникам за пределы компании. Обратите внимание, что при вводе информационной метки с клавиатуры сотрудники могут ошибаться и вводить между словами более 1 пробела или табуляции, а также писать название компании на русском языке, например, «ООО Demo Лаб», «ООО Демо Лаб».

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: печать

Проверить работоспособность.

Политика 13

В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу. Необходимо отслеживать следующие термины: COVID, COVID-19, коронавирус, коронавирусная инфекция.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: вирус

Проверить работоспособность.

Политика 14

Для защиты персональных данных сотрудников необходимо запрещать всем, кроме отдела кадров передавать информацию, содержащую данные паспортов (в том числе и сканы/фото), а также СНИЛС и ИНН.

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: пдн

Проверить работоспособность.

Политика 15

Необходимо контролировать передачу документов формата электронных таблиц (исключая csv файлы!), а также CAD-документации. Стоит учесть, что файлы могут передаваться в том числе и на съемных носителях информации.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Задание 16: Анализ инцидентов, обычные сводки

Создайте новую вкладку сводки в разделе «Сводка» под названием «Экзамен» и создайте в ней 4 виджета:

Динамика активности по событиям за последнюю неделю

Статистика по политикам за последние 7 дней

По типу событий: необработанные нарушения за три дня

По топ-нарушителям за текущий месяц.

Задание 17: Анализ инцидентов, специальные выборки

Необходимо создать новую вкладку в разделе «Сводка» под названием «Особые выборки» и добавить в нее виджеты:

Отображающий события с уровнем угрозы от низкого до высокого на правила копирования (внешние носители, печать) за последние 7 дней.

Отображающий события с любым одним тегом.

Модуль 4: Технологии анализа и защиты сетевого трафика, установка и конфигурирование

Описание

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.

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

Доступы и прочие данные указаны в дополнительной карточке задания

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

Задание 1: настройка сетевого окружения и компонентов систем

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 или Bridge, или сеть NAT для виртуального «Интернета» (в соответствии с инфраструктурой площадки, для связи всех координаторов между собой)

При работе на сервере виртуализации данные могут отличаться. Также при работе на сервере допускается создание дополнительной сети для обмена файлами, дистрибутивами, ключами между всеми ВМ.

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

IP адреса защищенных сетей (пример):

Центральный офис «Сеть 1 ЦО»: 192.168.100.0/24

Офис филиал «Сеть 1 Филиал»: 192.168.200.0/25

Офис сеть 2 «Сеть 2 Офис»: 172.16.2.0/26

Общий «Интернет» для всех координаторов: 10.20.30.0/27

Адреса выбираются самостоятельно из указанного диапазона.

Необходимо записать адреса, логины и пароли в текстовый файл vpn.txt.

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

Также могут понадобиться дополнительные компоненты, находящиеся в каталогах дистрибутивов.

Задание 1.1. Установка ПО Vpn Administrator для создания защищённой сети:

Установить СУБД на виртуальную машину WSRV-DB. При установке необходимо использовать смешанную аутентификацию (пользователь sa). Пароль БД установить 12345678.

Установить и настроить рабочее место администратора VPN (на базе виртуальной машины WSRV-NCC-1): Центр управления сетью (серверное и клиентское приложение ЦУС и УКЦ. Использовать ранее установленную базу данных на отдельном сервере.

Верным выполнением задания является установка базы данных на отдельный сервер.

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 на соответствующие виртуальные машины:

установить ПО VPN Client, рабочее место администратора;

Рабочее место администратора должно быть защищено токеном аутентификации. Необходимо настроить вход в систему по токену (ключу). Парольный вход должен быть отключен.

установить ПО VPN Coordinator;

установить ПО VPN Coordinator;

установить ПО VPN Client, рабочее место пользователя;

Необходимо зафиксировать процесс установки только скриншотами изменяемых вручную форм и скриншот первого запуска приложения.

Задание 1.3. Защита локально-вычислительной сети предприятия с применением ПО VPN

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.

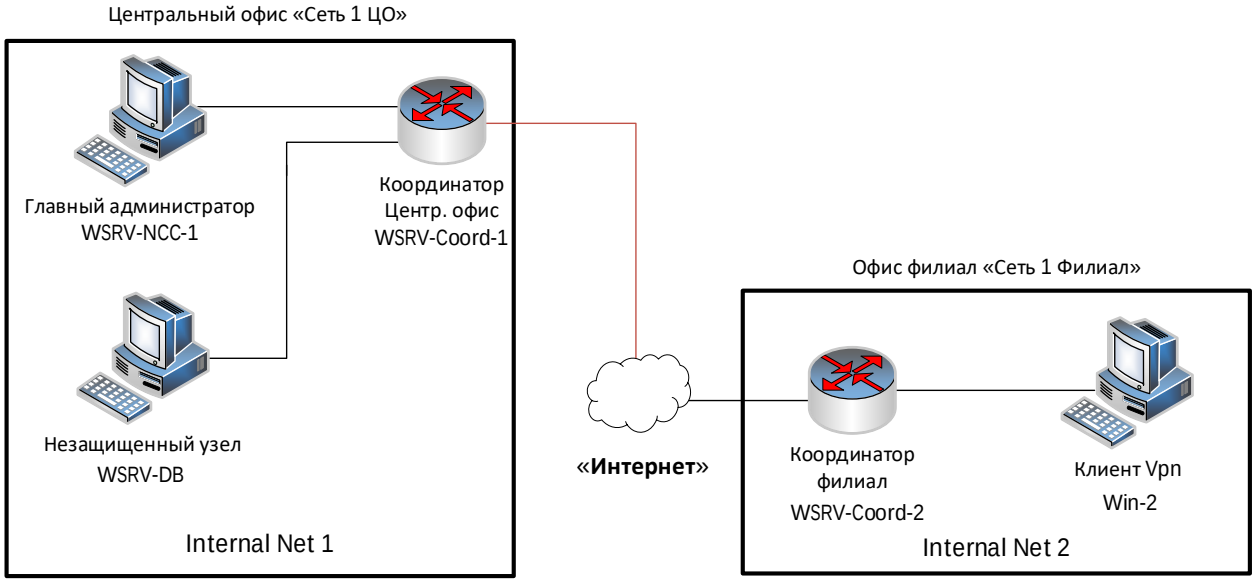


Рисунок 1 Схема защищенной сети

В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети и связи между ними (см. таблицу 1 и таблицу 2).

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

Вирт. машина	Название сетевого узла	ПО Vpn	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
WSRV-NCC-1	Главный администратор (VM) (защита токеном)	Vpn Administrator (ЦУС клиент и сервер + УКЦ) Vpn Client	ОС Server	Admin (защита токеном)
WSRV-DB	База данных (незащищенный узел)	—	ОС Server	—
WSRV-Coord-1	Координатор Центр Офис (VM)	Vpn Coordinator	ОС Server	CoordinatorOffice
WSRV-Coord-2	Координатор Филиал (VM)	Vpn Coordinator	ОС Server	CoordinatorSub

Win-2	Пользователь_2 Филиал (VM)	Vpn Client	ОС Pro	User2, минимальные полномочия

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	CoordinatorOffice	Admin	CoordinatorSub	user02
CoordinatorOffice	×	*	*	
Admin	*	×		*
CoordinatorSub	*		×	*
user02		*	*	×

Задание 1.4. 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, поменять тип паролей для пользователей («собственный»). Задать пароли пользователей и сохранить в текстовый файл. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить в папку на рабочем столе).

Создать группы узлов для центрального офиса 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 (на координаторах 2 интерфейса – внешний и внутренний), проверить доступность соседних узлов.

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

Стоит напомнить, что место администратора должно быть защищено токеном.

Задание 1.5. Модификация структуры защищенной сети

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

Модификация структуры сети:

- Добавить новый сетевой узел user01 и пользователя user01 за координатором ЦентрОфис (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем user02. На указанных узлах проверить появление нового узла.
- Добавить пользователя user02 на узле Пользователь_2 Филиал (Win-2 филиала), связать его со всеми пользователями группы узлов центральный офис и филиал. Для указанных пользователей проверить появление новой связи.
- Войти в Vpn клиент от данного пользователя на узле филиала.
- Отправить сообщение пользователю user01 с узла admin.
- зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:

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

Модуль 5: Технологии анализа и защиты сетевого трафика, компрометация, межсетевое взаимодействие и туннелирование

Задание 2.1. Компрометация узла защищенной сети

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя.

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

- скомпрометировать ключи пользователя user02 на узле Пользователь_2 Филиал
- произвести смену ключей пользователя и сетевых узлов,
- отправить обновления и произвести процедуру смены ключа пользователя на узле Пользователь_2 Филиал (фиксировать все шаги),
- войти от данного пользователя на узле филиала,
- проверить работу защищенной сети после обновления отправив сообщение от пользователя user02 администратору.

Восстановление взаимодействия с помощью ручной установки DST засчитано не будет.

Необходимо зафиксировать процесс настройки скриншотами или иным указанным способом.

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

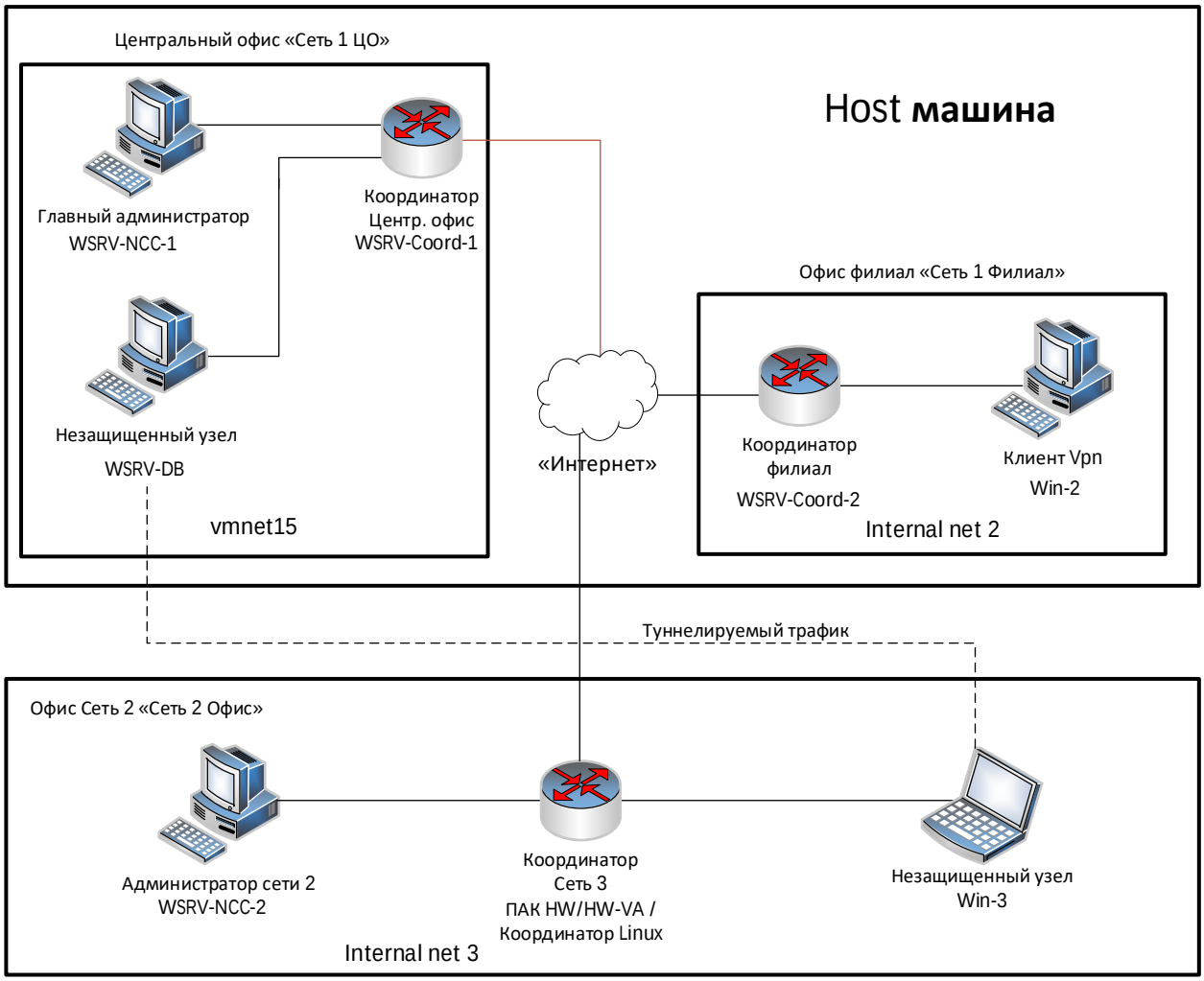


Рисунок 2 Схема межсетевого взаимодействия

Развернуть на WSRV-NCC-2 (Офис сеть 2 «Сеть 2 Офис») на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети:

- Рабочее место администратора (БД, ЦУС, УКЦ, Vpn Client)
- 1 координатор (ПАК HW или HV-VA, или координатор Linux в соответствии со структурой площадки). Допускается развертывание координатора windows (самостоятельным копированием виртуальной машины), но инициализация системы засчитана не будет.
- 1 узел Admin и пользователь Admin

Все пароли пользователей в сети Vpn сделать 12345678

Все пароли администраторов в сети Vpn сделать 12345678.

- Запустить координатор сети 2, настроить сеть в соответствии с заданием
- Настроить межсетевое между двумя защищёнными сетями взаимодействие с использованием асимметричного межсетевого мастер-ключа, сделать скриншоты всех этапов установки межсетевого взаимодействия.
- Проверить взаимодействие узлов, отправив сообщение узла Admin (сеть 1) на Admin (сеть 2).

Необходимо предоставить:

Файлы HTML структуры защищенной сети для обеих сетей после выполнения задания, скриншоты

Задание 2.3. Туннелирование в рамках межсетевого взаимодействия

- Подключить незащищенную машину в сети 3 (Win-3, без ПО Vpn).
- Для второй открытой машины использовать WSRV-DB в сети 1
- Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по шифрованному каналу. Проверить доступность незащищённых машин друг другу с помощью ICMP (ping), а также любым другим протоколом, например smb; проанализировать журналы IP-пакетов на координаторах.

Предоставить скриншоты выполнения.

5. Необходимые приложения

Приложение 1 Пояснения по подготовке площадки (документ docx)

Приложение 2 Карточка настроек сети и оборудования (документ docx)

Приложение 3 Эталонные файлы для выполнения заданий (архив zip)

Приложение 4 Пример пользователей и групп для домена (документ csv)

Примерный план работы[1] Центра проведения демонстрационного экзамена по КОД № 2.1 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

	Примерное время	Мероприятие
Подготовительный день	08:00	Получение главным экспертом задания демонстрационного экзамена
	08:00 – 09:00	Проверка готовности проведения демонстрационного экзамена, заполнение Акта о готовности площадки
	09:00 – 09:15	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение протоколов
	09:15 – 09:30	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах
	09:30 – 09:45	Регистрация участников демонстрационного экзамена
	09:45 – 10:15	Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	10:15 – 12:00	Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение протоколов
	12:00 – 16:00	Подготовка и/или проверка работоспособности площадки в соответствии с заданием
День 1	08:45 – 09:00	Ознакомление с заданием и правилами
	09:00 – 09:15	Брифинг
	09:15 – 11:15	Выполнение модуля 1
	11:15 – 11:30	Перерыв, обработка помещения, проветривание
	11:30 – 13:00	Выполнение модуля 2
	13:00 – 13:45	Обед, обработка помещения, проветривание
	13:45 – 15:15	Выполнение модуля 3
	15:15 – 15:30	Перерыв, обработка помещения, проветривание

[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.

	15:30– 17:00	Выполнение модуля 3
	16:30 – 19:00	Работа экспертов, заполнение форм и оценочных ведомостей
	19:00 – 20:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола Подготовка площадки для следующей экзаменационной группы (при наличии)
День 2	08:45 – 09:00	Ознакомление с заданием и правилами
	09:00 – 09:15	Брифинг
	09:15 – 10:45	Выполнение модуля 4
	10:45 – 11:00	Перерыв, обработка помещения, проветривание
	11:00 – 12:00	Выполнение модуля 4
	12:00 – 12:45	Обед, обработка помещения, проветривание
	12:45 – 14:15	Выполнение модуля 5
	14:15 – 14:30	Перерыв, обработка помещения, проветривание
	14:30– 16:00	Выполнение модуля 5
	16:00 – 18:00	Работа экспертов, заполнение форм и оценочных ведомостей
	18:00 – 19:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола Подготовка площадки для следующей экзаменационной группы (при наличии)

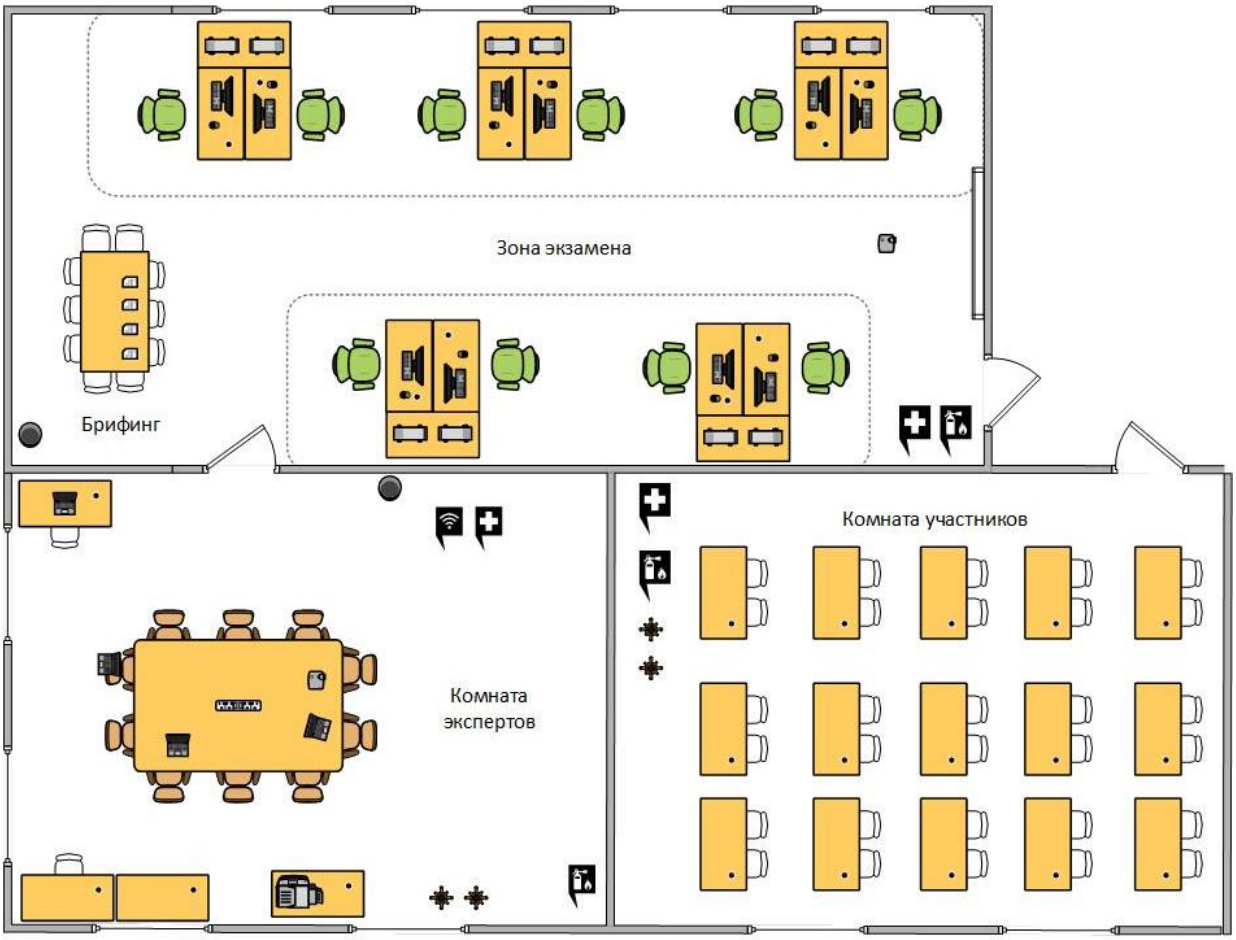
План застройки площадки для проведения демонстрационного экзамена по КОД № 2.1 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Номер компетенции: F7

Название компетенции: Корпоративная защита от внутренних угроз информационной безопасности

Общая площадь площадки: 100 м^2

План застройки площадки:



Приложения

Инфраструктурный лист для КОД № 2.1 (документ xlsx)

Пояснения по подготовке площадки для КОД № 2.1 (документ docx)

Карточка настроек сети и оборудования для КОД № 2.1 (документ docx)

Эталонные файлы для выполнения заданий для КОД № 2.1 (архив zip)

Пример пользователей и групп для домена для КОД № 2.1 (документ csv)