КОНКУРСНОЕ ЗАДАНИЕ

Региональные чемпионаты 2021-22

Сокращенное типовое задание – 85 баллов

Корпоративная защита от внутренних угроз информационной безопасности

Модуль 1, 3, 5
День 1

Менеджер компетенции: А.В. Сергеев

FUTURE SKILLS

Аннотация

Документ содержит типовое конкурсное задание 2021-22 региональных чемпионатов 2021-22 года по стандартам WorldSkills Russia по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности».

Конкурсное задание разработано на базе заданий Отборочных соревнований и IV Финала национального чемпионата Ворлдскиллс 2021 года. Практические задания собрали лучшие практические задачи в области обеспечения корпоративной безопасности в организациях реального сектора экономики и были апробированы на корпоративных чемпионатах ГК Росатом, ГК Роскосмос.

Использование документа печать (тиражом до 20 экз.) и распространение разрешено только в рамках организации и проведения региональных чемпионатов Ворлдскиллс. С вопросами и замечаниями можно обращаться по адресу: avsergeev@hse.ru

Состав рабочей группы по разработке типового КЗ:

- ***А.В Сергеев, менеджер компетенции,***
  НИУ ВШЭ, Москва;
- ***А.П. Бозров, сертифицированный эксперт,***
  ГБПОУ «Колледж связи № 54», Москва;
- ***А.А. Крылова, победитель МежВУЗ 2019,***
  ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Санкт-Петербург;
- ***А.В. Зябухина, эксперт-компатриот призёра ФНЧ 2021,***
  ГБПОУ КК "Краснодарский колледж электронного приборостроения", Краснодар;
- ***Н.В. Матвеев, сертифицированный эксперт,***
  ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Санкт-Петербург;
- ***Е.В. Трапезников, сертифицированный эксперт,***
  ФГАОУ ВО «Омский государственный технический университет» , Омск.

Дополнительные сведения (шаблон)

Общие сетевые настройки

Шлюз по умолчанию _____

DNS сервер провайдера _____

DNS сервер компании _____

Компьютер с виртуальными машинами:

Логин: ____ , пароль: ____

Документация находиться: _____

Дистрибутивы находиться: _____

Образы систем находятся: _____

Контроллер домена (DEMO.LAB):

IP адрес: _____Маска: _____

Домен: demo.lab

логин: _____ пароль: _____

DLP-система (IWTM)

Локальный вход: логин: root пароль: xxXX1234

IP адрес: _____ Маска: _____

Веб консоль логин: officer пароль: xxXX1234

Windows Server (IWDM):

Локальный вход: логин: admin пароль: xxXX1234

IP адрес: _____ Маска: _____

Windows 10 (Client 1):

Локальный вход: логин: admin пароль: xxXX1234

IP адрес: _____ Маска: _____

Проверка правил передачи через сайт dlptest.com

Модуль 1: Установка и настройка системы

Описание

Вы работаете инженером в центре информационной безопасности (департамент проектирования и внедрения) одного из интеграторов DEMO Lab.

Вам поручили собрать демонстрационный стенд в отдельной «песочнице» и настроить DLP-систему на отдельном сегменте сети.

В «песочнице» развернут контроллер домена (с каталогом Active Directory), с которым необходимо будет осуществить интеграцию DLP-системы. До настройки системы необходимо подготовить доменных пользователей.

В качестве виртуальной инфраструктуры для пилотного проекта используется среда виртуализации VMware Workstation.

В качестве DLP-системы выбран продукт InfoWatch Traffic Monitor (IWTM).

Вам необходимо установить и настроить компоненты DLP-системы в соответствии с выданным заданием.

Необходимо использовать следующие виртуальные машины:

- Demo (контроллер домена demo.lab)
- IWTM (предустановленный, необходимо настроить)
- Iwdm (Windows Server для IWDM, предустановленный)
- w10-cli1 (ПК первого нарушителя)
- w10-cli2 (ПК второго нарушителя)

Сетевые настройки виртуальных машин указаны в дополнительной карточке заданий.

Основными каналами потенциальной утечки данных являются носители информации, электронная почта и различные интернет-ресурсы.

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.

При выполнении заданий можно пользоваться справочными ресурсами в сети Интернет и документацией на компьютерах в папке «InfoWatch 6.11.5» на HDD.

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

Задание 1: Подготовка Active Directory

Примечание: *необходимо проверить, что данные пользователи уже не добавлены в Active Directory. Если добавлены, не выполнять повторно.*

Для дальнейших работ необходимо создать подразделение организации (Organization Unit) под названием «**Office**», добавить в него каталоги пользователей и компьютеров (Users и Computers).

В каталог Users необходимо добавить следующих пользователей:

- admin-dm (права доменного администратора, для машины iwdm)
- admin-bd (права доменного администратора, для машины db)
- tmofficer (права пользователя домена, для входа в веб-консоль iwtm)
- useroffice1 (1я машина нарушителя, права пользователя домена, w10-cli1)
- useroffice2 (2я машина нарушителя, права пользователя домена, w10-cli2)
- ldapuser (права пользователя домена, для всех ldap-синхронизаций)

Ваша задача – создать и настроить вышеперечисленных пользователей в соответствии с указанными условиями.

Для всех пользователей необходимо задать пароль xxXX1234

Настройте LDAP-синхронизацию для IWTM с помощью пользователя ldapuser.

Для работы с консолью IWTM используйте доменного пользователя tmofficer (задать все встроенные роли (officer и administrator) и все области видимости).

Стоит учесть, что после ввода в домен, компьютеры необходимо переносить в ранее созданный каталог Computers (внутри OU «Office»)

В соответствии с политикой компании для обеспечения безопасности компьютеров брандмауэр должен быть активен. Для установки компонентов системы необходимо настроить правила брандмауэра с помощью групповых политик домена.

Зайти пользователями useroffice1 на машину w10-cli1 и useroffice2 на машину w10-cli2.

Задание 2: Развертывание InfoWatch Crawler

Для контроля общих сетевых ресурсов в организации необходимо развернуть следующие сетевые компоненты InfoWatch Traffic Monitor на машину IWDM: Crawler Server и Crawler Scanner.

После установки InfoWatch Crawler необходимо создать задачу на ежедневное сканирование сетевых ресурсов (папки share_iwtm, share_iwdm). Предварительно требуется создать общие сетевые папки:

1. На виртуальной машине IWTM создать папку «share_iwtm» с правами чтения и записи для всех пользователей домена
2. На виртуальной машине IWDM создать папку «share_iwdm» с правами чтения и записи для всех пользователей домена

Зафиксировать создание и выполнение скриншотом.

Модуль 5: Технологии агентского мониторинга

Задание 1

Необходимо применить групповые политики Windows для OU «Office».

Групповая политика 1:

- Минимальная длина пароля должна составлять 8 символов;
- Срок жизни пароля должен составлять 25 дней
  Выполнение задания подтвердить скриншотами.

Групповая политика 2:

- Отключить возможность локального входа для пользователей tmofficer и ldapuser с помощью групповых политик
  Выполнение задания подтвердить скриншотами.

Групповая политика 3:

- С помощью редактора групповой политики запретить доступ к реестру. Выполнение задания подтвердить скриншотами.

Групповая политика 4:

- С помощью редактора групповой политики настройте запрет запуска winver.exe. Выполнение задания подтвердить скриншотами.

Групповая политика 5:

- С помощью редактора групповой политики ограничить доступ к панели управления. Выполнение задания подтвердить скриншотами.

Групповая политика 6:

- Задать Обязательный (Mandatory) профиль для пользователя useroffice2. Эталонный профиль можно сформировать с любого пользователя

Зафиксируйте все этапы настройки, создания и выполнения (срабатывание, где возможно) задания скриншотами в папке «Чемпионат» на рабочем столе компьютера.

Задание 2

Используйте для входа в консоль IWDM доменного пользователя *admin-dm*.

Задать максимальные права пользователя на работу в консоли IWDM.

Проверить работоспособность, зафиксировать настройку и выполнение скриншотом запущенной консоли.

Задание 3

Необходимо создать новые политики (кроме политики на устройства по

умолчанию),

Политика 1:

Название: «**Отдел 1**»

Группа компьютеров: Виртуальная машина пользователя userofficer1

Политика 2:

Название: «**Отдел 2**»

Группа компьютеров: Виртуальная машина пользователя userofficer2

Зафиксировать выполнение скриншотами.

Правила для **Отдела 1:**

Правило 1

Необходимо запретить создание снимков экрана в табличных процессорах (Excel или OpenOffice Calc) и калькуляторе для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2

Необходимо запретить печать на локальных принтерах, но при этом оставить возможность печати на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Правило 3

Создать политику по блокировке копирования исполняемых exe-файлов на USB-накопители. Проверить работоспособность и зафиксировать выполнение (зафиксировать результаты в виде скриншотов).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 4

В связи с небезопасностью ftp-серверов разрешить только скачивание по протоколу ftp, загрузку файлов на сервер запретить.

Проверить работоспособность на любом доступном файловом сервере и зафиксировать выполнение скриншотом.

Правила для **Отдела 2:**

Правило 5

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них. *Проверить работоспособность и зафиксировать выполнение скриншотом.*

Правило 6

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.*

Правило 7

На виртуальной машине необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP, а в группе компьютеров по умолчанию необходимо контролировать буфер обмена при копировании из/в терминальных сессий.

Проверить работоспособность попыткой копирования текста из сеанса RDP и зафиксировать выполнение скриншотом как блокировки, так и контроля. Для работы RDP может потребоваться дополнительная настройка.

Правило 8

Необходимо поставить на контроль буфер обмена в текстовых процессорах (Word или Writer или Wordpad).

Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики.

Правило 9

Для предотвращения неэффективного расхода рабочего времени сотрудников отслеживать движение видео контента (*.avi, *.mov, *.mp4) в общих папках компании. Отдельно контролировать файлы больше 10 Мбайт и меньше 10 Мбайт. (1 Мбайт = 1024 Кбайт)

Проверить работоспособность и зафиксировать выполнение скриншотом

Модуль 3: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Создайте в системе InfoWatch Traffic Monitor политики безопасности согласно нижеперечисленным заданиям.

- Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.
- Некоторые политики должны быть созданы с нуля, некоторые могут быть сделаны путём модификации существующих в системе.
- Для некоторых политик необходима работа с разными разделами консоли управления ТМ: 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, участник должен самостоятельно задать уровень угрозы при разработке политики).
- Списки сотрудников, занимаемые позиции и отделы сотрудников (HR, Accounting и др.) представлены в разделе «Персоны» Infowatch Traffic Monitor по результатам LDAP-синхронизации с AD-сервером компании
- После создания всех политик будет запущен автоматический «генератор трафика», который передаст на InfoWatch Traffic Monitor поток данных, содержащих как утечки, так и легальную информацию.
- При правильной настройке политики InfoWatch Traffic Monitor 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.
- В комплексных заданиях необходимо пользоваться объектами защиты.
- Задания можно выполнять в любом порядке.
- 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 на рабочем столе 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

ВНИМАНИЕ! Необходимо называть политики/объекты/категории/тэги и т.п. **ТОЛЬКО** в соответствии с номером и названием задания:

Политики — Политика XX, например «**Политика 5**». Для комбинированных политик формат: **Политика 5.1**, **Политика 5.2** и т.д.

Объект защиты — Объект и XX, например «**Объект 11**».

Ошибки в названиях приводят к снижению баллов или даже к невозможности проверки. При выполнении задания учитывайте, что совместно с созданными могут срабатывать стандартные политики, что необходимо предотвратить.

ВНИМАНИЕ! **ВСЕ политики «по-умолчанию»,** находящиеся в IWTM на момент старта соревнований**, должны быть отключены или удалены**

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

Задание 1

Создайте список веб-ресурсов и назовите его «Сайты партнеров». Туда необходимо включить следующие веб-ресурсы:
kb.infowatch.com, worldskills.moscow, worldskills.ru, infotecs.ru

Задание 2

Для правильной работы системы необходимо настроить периметр компании:
Домен: demo.lab.
Список веб ресурсов: Сайты партнеров
Группа персон: пользователи домена.
Исключить из перехвата почту генерального директора.
Подтвердите выполнение задания скриншотами.

Политика 1

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика (до ≈50%) как внутри компании, так и за ее пределы. Фотография котика есть в дополнительных данных.
Вердикт: Заблокировать ×
Уровень нарушения: низкий •
Тег: Политика 1

Политика 2

В последнее время бюджет компании стал резко падать. Подозрения пали на главного бухгалтера, директор подозревает его в проведении денежных средств «мимо кассы». В связи с этим необходимо отслеживать передачу всех номеров и сканов кредитных карт, отправляемых из отдела Бухгалтерии
Вердикт: Заблокировать ×
Уровень нарушения: высокий •
Тег: Политика 2

Политика 3

Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний. Критичными данными в выгрузке являются телефоны, ИНН, Регистрационный номер, ОКФС, ОКВЭД и ОКОПФ и в 1 документе присутствует более 5 компаний. Для настройки используйте файл stock_members_details_catch.csv.

Вердикт: Разрешить √

Уровень нарушения: низкий •

Тег: Политика 3

Политика 4

Дочерняя компания «ООО Повозка» занимается транспортировкой грузов в разные города. Каждому рейсу присваивается уникальный идентификационный номер по следующему шаблону «3 буквы (латиница, любой регистр) - (знак дефиса) номер груза (от 0 до 1000, исключая следующие номера: 777 и 315) - (дефис) от 1 до 3 букв (кириллица, верхний регистр) Например: jDT-123-Л , kSR-665-ЪГА Не должно быть срабатывания на следующие номера грузов (например: kdO-315-ю или jtfd-777-ШАП). Необходимо контролировать передачу, а также копирование на съемные носители и печать вышеуказанных данных. Проверить работоспособность. Учтите, что особо обобщенные регулярные выражения лучше разделить на несколько текстовых объектов для оптимизации поиска.

Вердикт: Разрешить √

Уровень нарушения: средний •

Тег: Политика 4

Политика 5

Необходимо создать политики для отслеживания документов (передача и копирование), содержащих договор компании (договор компании.docx).

Политики должны работать следующим образом (за периметр компании):

1. Если передается только договор компании (шаблон и заполненный шаблон, до 25% изменений) – разрешать передачу, уровень угрозы низкий, тег «Политика 5.1».
2. Если передается договор компании, в котором присутствует фамилия

генерального директора, а также главного бухгалтера – разрешать передачу, уровень угрозы средний, дополнительный тег «Политика 5.2». Политика не должна срабатывать, если в документе только фамилия директора или только фамилия бухгалтера.

3. Если передается договор компании, в котором присутствует фамилия генерального директора, главного бухгалтера, а также стоит печать компании (ООО Повозка) – разрешить передачу, уровень угрозы высокий, тег «Политика 5.3».

Проверить работоспособность. Политики не должны срабатывать внутри компании, только при передаче за периметр.

Все политики, объекты и прочие элементы должны называться в соответствии с номерами (например Объект 5.1, Политика 5.2, Технология 5.3 и т.д.)

Вердикт 1: Разрешить √

Уровень нарушения 1: низкий •

Тег 1: Политика 5.1

Вердикт 2: Разрешить √

Уровень нарушения 2: средний •

Тег 2: Политика 5.2

Вердикт 3: Заблокировать ×

Уровень нарушения 3: высокий •

Тег 3: Политика 5.3

Политика 6

Стало известно, что сотрудники охраны (Security) ООО «Повозка» за определенную сумму пропускают автомобили из близлежащих домов на служебную парковку. В связи с ужесточением корпоративной политики в компании, правом въезда на территорию обладает только генеральный директор.

Сотрудники охраны ведут журнал учета автомобилей в электронном виде и обмениваются между собой данными о припаркованных автомобилях.

Необходимо детектировать номера всех автомобилей, которые незаконно парковались на частной территории компании ООО «Повозка», исключая номер автомобиля генерального директора К333ОТ777.

Буквы, используемые в автомобильных номерах:

A, B, E, K, M, H, O, P, C, T, У, X (Верхний регистр)
Цифры, используемые в автомобильных номерах:
000 – 999
Регионы автомобильных номеров, подлежащие детектированию:
77, 97, 99, 177, 197, 199, 777, 799
Вердикт: заблокировать ×
Уровень нарушения: Высокий •
Тег: Политика 6

Политика 7

В честь юбилея компании была запущена акция с промокодами на скидку в 50% на перевозки для постоянных клиентов. По условиям акции промокод выдается только по запросу постоянного клиента. Есть вероятность утечки промокодов, в связи с этим необходимо контролировать защитить учечку текстового документа, содержащего промокоды («промокоды.docx»). Стоит учесть, что сотрудники могут воспользоваться жестким диском или флеш-накопителем, для того чтобы завладеть акционными купонами, а также слить не весь файл, а один или несколько купонов. Запретить передачу данных, содержащих информацию об этих купонах, а также отслеживать копирование этой информации на внешние носители, тег «Политика 7»
Проверить работоспособность на все купоны и на 1-2 купона.
Вердикт: заблокировать ×
Уровень нарушения: средний •
Тег: Политика 7

Политика 8

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела кадров отправлять сканы/скриншоты и документы, содержащие информацию о СНИЛС, ИНН, паспортных данных (в текстовом и графическом виде) за пределы компании.
Извлечение текстовых данных из сканированных документов, а также скриншотов подразумевает использование технологии OCR. Необходимо включить данную технологию (ABBYY), используя лицензию, которая

находится в папке дистрибутивов. (подробнее см. в доп. карточке задания)

Вердикт: заблокировать ×

Уровень нарушения: средний ●

Тег: Политика 8

Политика 9

Два месяца назад в компании DemoLab заметили, что сотрудница отдела кадров расходует в три раза больше бумаги, чем прежде, хотя объем работ не был увеличен. Путем наблюдения за сотрудницей было установлено, что она, состоя в совете школьной родительской общественности, регулярно собирает деньги с родителей за печать докладов и рефератов учеников класса, бесплатно распечатывая их в компании.

Необходимо создать политику безопасности, которая будет включать слова (с учетом морфологии): «реферат», «доклад», «ученик», «школа», «класс».

Проверку необходимо проверить путем отправки документа на печать и при помощи электронной почты.

Вердикт: Заблокировать ×

Уровень нарушения: низкий ●

Тег: Политика 9

Политика 10

В последнее время сотрудники стали чаще обсуждать популярные сериалы в мессенджерах и социальных сетях, из-за чего упала общая производительность на 5%. Было решено отследить, кто больше всего занимается не рабочей деятельностью, для чего необходимо создать политику для отслеживания 5 (пяти) популярных на данный момент сериалов при передаче через веб-сообщения и почту.

Список сериалов:

Ривердэйл, Сестра Рэтчед, Племена Европы, Сквозь снег, Варвары

Вердикт: разрешить √

Уровень нарушения: низкий ●

Тег: Политика 10

Политика 11

Оказалось, что сотрудники не только обсуждают сериалы, а еще и обмениваются ссылками и torrent-файлами для их скачивания, после чего скачивают их, используя интернет-канал компании или обмениваются скачанным материалом внутри компании, что также нагружает сеть и заполняет ненужными данными локальные диски пользователей.

В связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов формата .torrent и ссылок формата `magnet:` (и содержащей urn (хеш) файла). Ложных срабатываний просто на слово Magnet (в т.ч. с двоеточием) быть не должно.

Стоит учесть, что magnet-ссылки могут передаваться в том числе через буфер обмена в пределах браузера Google Chrome.

Вышеуказанными данными сотрудники могут обмениваться не только внутри компании.

Для торрент-файлов и ссылок:

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: Политика 11

Политика 12

У директора компании скоро юбилей и сотрудники решили его поздравить, сделав коллаж из его фотографий. Для того чтобы данное поздравление не попало к директору раньше срока, необходимо контролировать передачу фотографий директора, как внутри компании, так и за его пределами. Критичным является минимум 20%-ное совпадение передаваемого фото.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: Политика 12

Политика 13

При переезде в новый просторный офис, компанией ООО Demo Lab был расширен штаб сотрудников – было решено взять несколько десятков выпускников технических вузов на стажировку. Для того, чтобы они работали более эффективно, директор компании предложил отслеживать доступ

сотрудникам, работающим в отделе ИТ, доступ к основным социальным сетям и анонимным имиджбордам – vk.com, ok.ru, t.me, dobrochan.org, ii.yakuji.moe
Контроль для тестовых целей установить за электронными письмами в эти доменные зоны.
Вердикт: разрешить √
Уровень нарушения: средний •
Тег: Политика 13

Политика 14
Сотрудники и партнеры компании стали получать большое количество различных рекламных сообщений на мобильные номера, в связи с чем возникло подозрение о том, что кто-то производит «слив» номеров из баз данных компании путем передачи информации за пределы компании через браузер, почту или флешки.
Необходимо контролировать передачу как минимум 3 мобильных номеров в 1 сообщении, т.к. передача всего одного номера не является потенциальным сливом данных (может быть просто контактной информацией).
Мобильные номера могут быть только операторов РФ (код страны 7, код оператора начинается с 9), в различных форматах, например:
+7 (987) 123-45-67, +79871234567, +7 987 123 4567, 8-987 123-4567 и т.д.
Необходимо учесть все варианты, в т.ч. без кода страны, кода выхода на городскую телефонную сеть, комбинации пробелов, скобок, дефисов.
Вердикт: разрешить √
Уровень нарушения: Высокий •
Отправить уведомление: офицеру безопасности
Тег: Политика 14

Политика 15
Необходимо поставить на мониторинг все зашифрованные и запароленные данные, так как попытки передачи таких данных несут потенциальную опасность утечки.
Проверить работоспособность.
Вердикт: разрешить √
Уровень нарушения: низкий • **Тег:** Политика 15