Таблица 1 – Данные техники по сценарию атаки

Этап Mitre	Техника Mitre
Получение учетных данных	T1003. OS Надежный сброс
Подготовка ресурсов	T1583.002. DNS Сервер
Первоначальный доступ	T1190. Эксплуатация программного обеспечения, предназначенного для использования в общественных целях
Сбор данных	T1560. Архивированные данные
Подготовка ресурсов	T1584.005. Ботнет
Первоначальный доступ	T1566. Фиширование
Предотвращение обнаружения	T1553. Субвертирование целевых фондов
Первоначальный доступ	T1189. Проезжай мимо Компромисы
Перемещение внутри периметра	T1021.001. Протокол дистанционного рабочего стола

Таблица 2 – Вывод наиболее опасных сочетаний уязвимость - техника

Техника Mitre	ID уязвимости	Описание уязвимости
T1560. Архивированные данные	-	-
T1584.005. Ботнет	-	-
T1189. Проезжай мимо Компромисы	-	-
T1553. Субвертирование целевых фондов	-	-
T1021.001. Протокол дистанционного рабочего стола	-	-
T1583.002. DNS Сервер	-	-
T1566. Фиширование	CVE-2016-2496	Создание диалога разрешения UI в Android 6.x до 2016 06 01 позволяет нападавшим совершать атаки и получать доступ к произвольным частным файлам хранения, создавая частично перекрывающееся окно, а также внутренний жучок 26677796.

T1566. Фиширование	CVE-2021-43048	Интернэшнл Сервер и Gateway Server компоненты TIBCO Software Inc. содержат уязвимость, которая теоретически позволяет неподтверждённому нападающему с доступом к сети осуществить атаку на пострадавшую систему. Для успешного нападения с использованием этой уязвимости не требуется взаимодействие человека от другого человека, кроме нападающего. Затрагиваемыми релизами являются TIBCO Software Inc. TIBCO Partnership Express: версии 6.2.1 и ниже.
T1566. Фиширование	CVE-2020-0387	В декларативных файлах пакета SmartSpace, возможно, есть вектор крана из-за отсутствия проверки разрешения. Это может привести к местной эскалации привилегий и угона счетов без дополнительных прав на исполнение. Для эксплуатации требуется взаимодействие пользователей. Продукт: AndroidVersion: Android ID ядра Android: A 156046804
T1566. Фиширование	CVE-2021-0302	В BookInstaller возможна атака, вызванная ненадежным значением по умолчанию. Это может привести к местной эскалации привилегий и разрешений, не требующих дополнительных прав при исполнении. Для эксплуатации требуется взаимодействие пользователей. Продукт: AndroidVersions: Android 8.1 Android 9 Android 10 Android ID: A 155287782
T1566. Фиширование	CVE-2021-0305	В BookInstaller возможна атака, вызванная ненадежным значением по умолчанию. Это может привести к местной эскалации привилегий и разрешений, не требующих дополнительных прав при исполнении. Для эксплуатации требуется взаимодействие пользователей. Продукт: AndroidVersions: Android 8.1 Android 9 Android 10 Android ID: A 15401544

T1566. Фиширование	CVE-2021-39692	В программе SetupLayoutActivity.java есть возможный способ установить рабочий профиль, обойдущий согласие пользователя из-за атаки на кран/наклад. Это может привести к местной эскалации привилегий при наличии прав пользователя на исполнение. Для эксплуатации необходимо взаимодействие пользователей. Продукт: AndroidVersion: Android 10 Android 11 Android 12 Android ID: A 20961139
T1566. Фиширование	CVE-2021-39702	На сайте Create of ProquestManageCredentials.java есть возможный способ для приложения третьей стороны установить сертификаты без одобрения пользователя из-за атаки на кран/наклад. Это может привести к местной эскалации привилегий при наличии прав пользователей на исполнение. Для эксплуатации необходимо взаимодействие пользователей. Продукт: AndroidVersions: Android 12 Android ID: A 205150380
T1566. Фиширование	CVE-2020-0394	В OnCreate of BluetoothPairingDialog.java, возможно, есть вектор крана из-за ненадежного значения по умолчанию. Это может привести к местной эскалации привилегий и ненадежных устройств, позволяющих получить доступ к спискам контактов без дополнительных прав на исполнение. Для эксплуатации необходимо взаимодействие пользователей. Продукт: AndroidVersions: Android 8,0 Android 8.1 Android 9 Android 10 Android 11 Android ID: A 15548639
T1566. Фиширование	CVE-2021-0487	На сайте CalenterDebugActivity.java существует возможный способ экспортировать календарь данных в Sdcard без согласия пользователя из-за атаки на календарь. Это может привести к местной эскалации привилегий с необходимыми привилегиями в исполнении пользователей. Взаимодействие пользователей не является необходимым для эксплуатации. Продукт: AndroidVersions: Android 11 Android ID: A 174046397

T1566. Фиширование	CVE-2021-1040	На сайте BluetoothPairingSelectiveFragment.java, возможно, есть EoP из-за атаки на ткацкие/накладные. Это может привести к местной эскалации привилегий при отсутствии дополнительных прав на исполнение. Для эксплуатации необходимо взаимодействие пользователей. Продукт: AndroidVersions: Android 10 Android 11 Android 12 Android 9 Android ID: A 182810085
T1190. Эксплуатация программного обеспечения, предназначенного для использования в общественных целях	-	-
T1003. OS Надежный сброс	CVE-2021-1361	Уязвимость в создании внутренней службы управления файлами для Cisco Nexus 3 000 Series Smitts и Cisco Nexus 9000 Series Strottes в автономном режиме NX OS, который работает с Sisco NX OS Software, может позволить неподтверждённому, удаленному нападающему создать, удалить или перезаписать произвольные файлы с корневыми привилегиями на устройстве. Эта уязвимость существует потому, что TCP порт 9075 неправильно настроен на то, чтобы слушать и отвечать на запросы о внешнем подключении. Нападающий может использовать эту уязвимость, отправив сфабрикованные пакеты TCP на IP-адрес, который расположен на локальном интерфейсе в порту TCP 9075. Успешная эксплуатация может позволить нападающему создать, удалить или переписать произвольные файлы, включая чувствительные файлы, связанные с конфигурацией устройства. Например, нападавший мог бы добавить пользовательский счет без ведома администратора устройства.
T1003. OS Надежный сброс	CVE-2015-5211	В некоторых ситуациях Spring Framework 4.2.0 - 4.2.1, 4.0,0 - 4.1.7, 3.2.0 - 3.2.14 и более старые неподтвержденные версии уязвимы к атаке отражаемого файла (RFD). Это нападение связано с злонамеренной разработкой пользователем URL с расширенным пакетным скриптом, что приводит к скачиванию ответа, а не к его передаче, и включает также некоторые вводимые данные, отраженные в ответе.

T1003. OS Надежный сброс	CVE-2019-13404	Установщик MSI для Python до 2,7.16 на Windows по умолчанию к каталогу C:\Python27, который упрощает для местных пользователей ввод троянского лошадиного кода. (Это также влияет на старые релизы 3.x до 3.5.) ПРИМЕЧАНИЕ: позиция поставщика заключается в том, что пользователь обязан обеспечить контроль доступа C:\Python27 или выбрать другой каталог, потому что для обратной совместимости требуется, чтобы C:\Python27 оставался по умолчанию для 2,7.x
T1003. OS Надежный сброс	CVE-2022-27837	Уязвимость с использованием PendingIntent in Disability до версии 12.5.3.2 в Android R(11.0) и 13.0.1.1 в Android S(12.0) позволяет нападавшему получить доступ к файлу с системной привилегией.
T1003. OS Надежный сброс	CVE-2020-3927	Произвольная уязвимость доступа к файлам существует в ServiSign Security bigin, пока нападавшие узнают о конкретной функции API, они могут получить доступ к произвольным файлам в целевой системе с помощью выбранного параметра API.
T1003. OS Надежный сброс	CVE-2017-11746	Tenshi 0,15 создает файл 10si.pid после отказа от привилегий на некоренный счет, который может позволить местным пользователям уничтожить произвольные процессы, используя доступ к этому некорневому счету для десятиши.pid модификацию до того, как корневой сценарий выполнит команду "Kill "cat/pathame/tenshi.pid".
T1003. OS Надежный сброс	CVE-2020-3926	Произвольная уязвимость доступа к файлам существует в ServiSign Security bigin, пока нападавшие узнают о конкретной функции API, они могут получить доступ к произвольным файлам в целевой системе с помощью выбранного параметра API.
T1003. OS Надежный сброс	CVE-2020-11469	Клиент на собраниях через 4,6.8 на копиях acOS, свернутых в пользовательский временный каталог во время установки, что позволяет локальному процессу (с привилегиями пользователя) получить доступ к корневому коду путем замены рулонного листа.

T1003. OS Надежный сброс	CVE-2021-22015	Сервер vCenter содержит множество факторов уязвимости к эскалации местных привилегий из-за неправильного разрешения файлов и справочников. Удостоверенный местный пользователь с неадминистративной привилегией может использовать эти вопросы для повышения своих привилегий, чтобы заложить основу на vCenter Server Appliance.
T1003. OS Надежный сброс	CVE-2022-24138	IOBit Advanced System Care (Asc.exe) 15 и Action Center Cload оба компонента IOBit annuaire в папку программных данных, папка программных данных имеет разрешения "rwx" для непривилегированных пользователей. Недостаточные пользователи могут использовать SetOpLock, чтобы дожидаться создания Процесса и переключить подлинный компонент со злоумышленным исполнением, тем самым приобретая кодовое исполнение в качестве высокопривилегированного пользователя (Low Privilege > High Secretity ADMIN).

Таблица 3 – Объекты защиты

ID объекта	ID техники	ID уязвимости	Название объекта защиты
O1	1560. Архивированные данные	-	Устройство хранения данных
O2	1584.005. Ботнет	-	Обеспечивающие системы
O2	1021.001. Протокол дистанционного рабочего стола	-	Обеспечивающие системы
O2	1566. Фиширование	CVE-2021-43048	Обеспечивающие системы
O3	1189. Проезжай мимо Компромисы	-	Средства защиты информации
O3	1003. OS Надежный сброс	CVE-2015-5211	Средства защиты информации
O3	1003. OS Надежный сброс	CVE-2019-13404	Средства защиты информации
O3	1003. OS Надежный сброс	CVE-2022-27837	Средства защиты информации
O3	1003. OS Надежный сброс	CVE-2020-3927	Средства защиты информации
O3	1003. OS Надежный сброс	CVE-2017-11746	Средства защиты информации
O3	1003. OS Надежный сброс	CVE-2020-3926	Средства защиты информации
O3	1003. OS Надежный сброс	CVE-2020-11469	Средства защиты информации
O3	1003. OS Надежный сброс	CVE-2021-22015	Средства защиты информации
O3	1003. OS Надежный сброс	CVE-2022-24138	Средства защиты информации

O4	1553. Субвертирование целевых фондов	-	Автоматизированное рабочее место
O5	1583.002. DNS Сервер	-	Периферийное оборудование
O5	1003. OS Надежный сброс	CVE-2021-1361	Периферийное оборудование
O6	1566. Фиширование	CVE-2016-2496	Информация (данные), содержащаяся в системах и сетях
O6	1566. Фиширование	CVE-2020-0387	Информация (данные), содержащаяся в системах и сетях
O6	1566. Фиширование	CVE-2021-0302	Информация (данные), содержащаяся в системах и сетях
O6	1566. Фиширование	CVE-2021-0305	Информация (данные), содержащаяся в системах и сетях
O6	1566. Фиширование	CVE-2021-39692	Информация (данные), содержащаяся в системах и сетях
O6	1566. Фиширование	CVE-2021-39702	Информация (данные), содержащаяся в системах и сетях
O6	1566. Фиширование	CVE-2020-0394	Информация (данные), содержащаяся в системах и сетях
O6	1566. Фиширование	CVE-2021-0487	Информация (данные), содержащаяся в системах и сетях
O6	1566. Фиширование	CVE-2021-1040	Информация (данные), содержащаяся в системах и сетях
O7	1190. Эксплуатация программного обеспечения, предназначенного для использования в общественных целях	-	Сервер

Таблица 4 – Модель нарушителя

ID нарушителя	Тип нарушителя	Техника MITRE	ID уязвимости	ID объекта	Мотивация нарушителя
N1	Авторизованные пользователи систем и сетей	T1560. Архивированные данные	-	O1	Кража данных, нарушение политики
N1	Авторизованные пользователи систем и сетей	T1189. Проезжай мимо Компромисы	-	O3	Кража данных, нарушение политики
N2	Поставщики вычислительных услуг и услуг связи	T1584.005. Ботнет	-	O2	Неосторожность, ошибка, влияние третьих лиц

N2	Поставщики вычислительных услуг и услуг связи	T1190. Эксплуатация программного обеспечения, предназначенного для использования в общественных целях	-	O7	Неосторожность, ошибка, влияние третьих лиц
N3	Лица, обеспечивающие поставку программных и программно-аппаратных средств	T1021.001. Протокол дистанционного рабочего стола	-	O2	Конкуренция, финансовая выгода, влияние служб
N4	Физическое лицо (хакер)	T1566. Фиширование	CVE-2021-43048	O2	Любопытство, самореализация, идеологические убеждения
N4	Физическое лицо (хакер)	T1003. OS Надежный сброс	CVE-2015-5211	O3	Любопытство, самореализация, идеологические убеждения
N4	Физическое лицо (хакер)	T1553. Субвертирование целевых фондов	-	O4	Любопытство, самореализация, идеологические убеждения
N4	Физическое лицо (хакер)	T1566. Фиширование	CVE-2016-2496	O6	Любопытство, самореализация, идеологические убеждения
N4	Физическое лицо (хакер)	T1566. Фиширование	CVE-2020-0387	O6	Любопытство, самореализация, идеологические убеждения
N4	Физическое лицо (хакер)	T1566. Фиширование	CVE-2021-0302	O6	Любопытство, самореализация, идеологические убеждения
N4	Физическое лицо (хакер)	T1566. Фиширование	CVE-2021-0305	O6	Любопытство, самореализация, идеологические убеждения
N4	Физическое лицо (хакер)	T1566. Фиширование	CVE-2021-39692	O6	Любопытство, самореализация, идеологические убеждения

N4	Физическое лицо (хакер)	T1566. Фиширование	CVE-2021-39702	O6	Любопытство, самореализация, идеологические убеждения
N4	Физическое лицо (хакер)	T1566. Фиширование	CVE-2020-0394	O6	Любопытство, самореализация, идеологические убеждения
N4	Физическое лицо (хакер)	T1566. Фиширование	CVE-2021-0487	O6	Любопытство, самореализация, идеологические убеждения
N4	Физическое лицо (хакер)	T1566. Фиширование	CVE-2021-1040	O6	Любопытство, самореализация, идеологические убеждения
N5	Системные администраторы и администраторы безопасности	T1003. OS Надежный сброс	CVE-2019-13404	O3	Саботаж, кража данных, внедрение уязвимостей
N6	Преступные группы	T1003. OS Надежный сброс	CVE-2022-27837	O3	Финансовая выгода, организованная преступность
N6	Преступные группы	T1003. OS Надежный сброс	CVE-2020-3927	O3	Финансовая выгода, организованная преступность
N6	Преступные группы	T1003. OS Надежный сброс	CVE-2017-11746	O3	Финансовая выгода, организованная преступность
N6	Преступные группы	T1003. OS Надежный сброс	CVE-2020-3926	O3	Финансовая выгода, организованная преступность
N6	Преступные группы	T1003. OS Надежный сброс	CVE-2020-11469	O3	Финансовая выгода, организованная преступность
N6	Преступные группы	T1003. OS Надежный сброс	CVE-2021-22015	O3	Финансовая выгода, организованная преступность
N6	Преступные группы	T1003. OS Надежный сброс	CVE-2022-24138	O3	Финансовая выгода, организованная преступность

N7	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	T1583.002. DNS Сервер	-	O5	Месть, небрежность, ошибка
N8	Разработчики программных и программно-аппаратных средств	T1003. OS Надежный сброс	CVE-2021-1361	O5	Внедрение уязвимостей, шпионаж, финансовая выгода

Таблица 5 – Меры обнаружения инцидентов относительно техники

id Техники	id Меры	Название меры обнаружения	Рекомендации обнаружения и регистрации
T1560	DS0017	Выполнение команд	Отслеживайте выполненные команды и аргументы в пользу действий, которые помогут в сжатии или шифровании данных, собранных до эксфильтрации, таких, как смола.
T1560	DS0022	Создание файла	Мониторинг новых файлов, написанных с дополнениями и/или заголовками, связанными с сжатыми или зашифрованными типами файлов.
T1560	DS0009	Создание процессов	Мониторинг новых процессов и/или командных линий, которые помогают в сжатии или шифровании данных, собираемых до эксфильтрации, таких, как 7 Zip, WinRAR и WinZip.
T1560	DS0012	Скриптовая казнь	Контроль за любыми попытками создать скрипты в системе будет считаться подозрительной. Если скрипты не используются в системе, а используются, то скрипты, выходящие из цикла выполнения функций администратора, вызывают подозрение. Скрипты следует, по возможности, забирать из файловой системы для определения их действий и намерений.
T1189	DS0015	Содержание журнала приложения	Файрволы и прокси могут инспектировать URL по потенциально известным плохим доменам или параметрам. Они также могут проводить репутацию, основанную на анализе на веб-сайтах и их запрашиваемых ресурсах, таких как возраст домена, на кого он зарегистрирован, если он в известном плохом списке, или сколько других пользователей подключено к нему раньше.
T1189	DS0022	Создание файла	Монитор для новых файлов, написанных на диск, чтобы получить доступ к системе через пользователя, посещающего веб-сайт в обычном порядке просмотра.

T1189	DS0029	Создание сетевых связей	Отслеживание новых сетевых подключений к неподтвержденным узлам, которые используются для отправки или получения данных.
T1189	DS0029	Содержание сетевых потоков	Наблюдение за другими необычными сетевыми потоками, которые могут указывать на дополнительные инструменты, переданные в систему. Используйте сетевые системы обнаружения проникновения, иногда с инспектированием SSL/TLS, для поиска известных злонамеренных сценариев (разведка, разбрызгивание и идентифицирующие скрипты браузера часто используются повторно), общего скрипта закулисного и эксплуатационного кода.
T1189	DS0009	Создание процессов	Ищите поведение в системе конечных точек, которое может указывать на успешный компромисс, например аномальное поведение браузеров. Это может включать подозрительные файлы, написанные на диск, доказательства впрыскивания Процесса для попыток скрыть исполнение, или доказательства Discovery.
T1553	DS0017	Выполнение команд	Мониторинг команд может выявлять злонамеренные попытки изменения параметров доверия, такие, как установка корневых сертификатов или модификация параметров/стратегий доверия, применяемых к файлам.
T1553	DS0022	Метаданные файла	Собирает и анализирует метаданные о подписании сертификатов на программном обеспечении, которое выполняет в рамках окружающей среды в целях выявления необычных характеристик сертификатов и их выпадов.
T1553	DS0022	Модификация файла	Периодически регистрируемые SIP и трастовые провайдеры (регистрационные записи и файлы на диске), в частности в поисках новых, модифицированных или не связанных с Microsoft записей[1] Также анализируют данные Autoruns на странности и аномалии, особенно злоумышленные файлы, пытающиеся обеспечить непрерывное исполнение путем сокрытия в местах запуска автомобилей. Авторуны будут скрывать записи, подписанные Microsoft или Windows по умолчанию, поэтому проследуйте за тем, чтобы "Hide Microsoft Entries" и "Hide Windows Entries" были выбраны.[1] On macos, удаление флага комapple. qarantine пользователя вместо операционной системы является подозрительным действием и должно быть дополнительно изучено.

T1553	DS0011	Загрузка модуля	Позволить CryptoAPI v2 (CAPI) регистрировать события [7] для мониторинга и анализа ошибок, связанных с неудавшейся проверкой достоверности данных о доверии (Event ID 81, хотя это событие может быть подорвано угнанными компонентами доверительных поставщиков), а также любыми другими представленными информационными событиями (например: успешные подтверждения). Заготовка данных о добросовестности может также служить ценным показателем злоумышленных SIP или нагрузки доверительных поставщиков, поскольку защищенные процессы, пытающиеся загрузить злонамеренно сфабрикованный компонент подтверждения достоверности данных о доверии, скорее всего, не сработают (Event ID 3033). [1]
T1553	DS0009	Создание процессов	Отслеживание процессов и доводов в пользу злонамеренных попыток изменить параметры доверия, таких, как установка корневых сертификатов или модификация параметров доверия/стратегии, применяемых к файлам.
T1553	DS0024	Создание ключей регистрации Windows	Контроль за созданием (суб) ключей в регистре Windows может вскрыть злоумышленные попытки изменить параметры доверия, такие как установка корневых сертификатов. Закрепленные корневые сертификаты находятся в регистре под No HKLM\SOFTVARE\Microsoft_EnterpriseCertificates\Root\Certificates\ и [HKLM или HKCU]\Software[\Policies]\Microsoft_SystemCertificates\Root\Certificates\. Существует подгруппа корневых сертификатов, которые согласуются между системами Windows* 18F7C1FC390203FA2861A7BA5* 7F88CD7223F398A390FA390FEDEDEDEADEADEA393396369330DFEADEAEASA373737373733ASA3A350A335* 788CDC7223C383199431934343434C369FFFFE*
T1553	DS0024	Модификация ключа регистрации Windows	Мониторинг изменений в регистре Windows может вскрывать злоумышленные попытки изменить параметры доверия, такие как установка корневых сертификатов. Закрепленные корневые сертификаты находятся в регистре под No HKLM\SOFTWARE\Microsoft_EnterpriseCertificates\Root_Certificates_ и [HKLM или HKCU]\Software[\Policies]\Microsoft\SystemCertificates\. Существует подгруппа корневых сертификатов, которые согласуются между системами Windows и могут использоваться для сравнения: [8] Кроме того, рассмотреть вопрос о том, чтобы дать возможность Глобальной аудиторской проверке доступа к регистру [9] в рамках политики усовершенствованной проверки безопасности применять контрольный список доступа к глобальной системе (SACL) и аудитировать события, связанные с модификацией значений регистра (sub) ключей, связанных с SIP и доверенными поставщиками: [10]

T1021.001	DS0028	Создание сериала Logon	Monitor for user accounts included in systems, связанных с RDP (ex: Windows EID 4624 Logon Type 10). Другие факторы, такие, как схемы доступа (ex: несколько систем за относительно короткий период времени) и активность, происходящая после удаленного входа в систему, могут указывать на подозрительное или злонамеренное поведение с RDP. Monitoring Logon and Logoff activers for Hosts in the Secretation of situation. Эта информация может использоваться в качестве индикатора необычной деятельности, а также в качестве подтверждения деятельности, наблюдаемой в других местах.
T1021.001	DS0028	Метаданные о сериале " Logon session " (< < Сеанс > >)	Монитор аутентификационных журналов и анализа необычных схем доступа. Удалённый локон рабочего стола, через RDP, может быть типичным для системного администратора или ИТ-поддержки, но только с отдельных рабочих станций. Мониторинг удаленных логарифмов рабочего стола и сопоставление с известными/утвержденными системами происхождения могут обнаружить боковое перемещение противника. Analytic 1 sourcetytype = "WinEventLog: Security" Code ="4624" и "LogonType="10" и "AutentificationPackageName"= "Negotiate" и TargetUserName="Admin*")
T1021.001	DS0029	Создание сетевых связей	Монитор новых сетевых подключений (как правило, через порт 3389), которые могут использовать Value Accounts для регистрации в компьютере с помощью дистанционного протокола рабочего стола (RDP). Затем противник может совершать действия в качестве регистрации пользователя. Другие факторы, такие, как схемы доступа и активность, которые возникают после удаленного входа, могут указывать на подозрительное или злонамеренное поведение с RDP.Analytic 1 Abreal RDP Network Connections Sourcuts sources = zeeek / поиск dest_port=3389 /// Fair RDP stats подсчёт frc_ip, dest_ip, dest_ports, где src_ip!= "trusted_ips" AND dest_ip!= "Internal_Servers"
T1021.001	DS0029	Сетевой поток	Отслеживание потоков необычных данных, которые могут использовать действительные счета для регистрации в компьютере с помощью дистанционного рабочего стола (RDP). Протокол дистанционного рабочего стола (RDP), встроенный в операционные системы Microsoft, позволяет пользователю удаленно зарегистрироваться на рабочем столе другого хоста. Он позволяет интерактивному доступу к окнам и переднему доступу к клавишам, кликам мыши и т.д. Сетевые администраторы, энергопользователи и конечные пользователи могут использовать RDP для повседневных операций. С точки зрения противника RDP предоставляет средство для бокового перемещения к новому хосту. Определение того, какие соединения RDP соответствуют противостоящей деятельности, может быть трудной проблемой в высокодинамичных условиях, но будет полезно для определения масштабов компромисса.

T1021.001	DS0009	Создание процессов	Monitor for regional process (например, mstsc.exe), который может использовать Daily Accounts для регистрации в компьютере с помощью дистанционного протокола рабочего стола (RDP). Затем противник может осуществлять действия, которые порождают дополнительные процессы, в качестве регистрироваться на пользователе.
T1566	DS0015	Содержание журнала приложения	Мониторинг для регистрации, передачи и/или других артефактов третьих сторон, которые могут отправлять сообщения о фишинге для получения доступа к системам жертв. Фильтрация на основе DKIM+SPF или анализа заголовков может помочь обнаружить, когда отправитель электронной почты спуфирован.[17] [18] проверка URL в электронной почте (включая расширение сокращенных ссылок) может помочь обнаружить ссылки, ведущие к известным злоумышленным сайтам. Детонационные камеры могут использоваться для обнаружения этих ссылок и либо автоматически отправиться на эти сайты для определения того, являются ли они потенциально злоумышленными, или же ждать и фиксировать контент, если пользователь посещает ссылку. Монитор звонит по журналам из корпоративных устройств для идентификации схем потенциального голосового шишинга, таких как звонки или звонки с известных злоумышленных номеров телефона. Корректировать эти записи с системными событиями.
T1566	DS0022	Создание файла	Отслеживайте новые файлы из фишинг-сообщений, чтобы получить доступ к системам жертв.
T1566	DS0029	Содержание сетевых потоков	Мониторинг и анализ структуры движения SSL/TLS и проверки пакетов, связанных с протоколом (протоколами), которые не соответствуют ожидаемым стандартам протокола и транспортным потокам (например, посторонние пакеты, не относящиеся к установленным потокам, бесплатные или аномальные транспортные потоки, аномальные синтаксии или структура).
T1566	DS0029	Сетевой поток	Мониторинг сетевых данных для необычных потоков данных. Процессы с использованием сети, которая обычно не имеет сетевой связи или никогда ранее не была замечена, вызывают подозрение.
T1190	DS0015	Содержание журнала приложения	Обнаружение программного обеспечения может быть сопряжено с трудностями в зависимости от имеющихся инструментов. Использование программного обеспечения может не всегда быть успешным или может привести к нестабильности процесса эксплуатации или к катастрофе. < < Программное обеспечение > > может выявлять неправильные вводимые данные, пытающиеся использовать. < < Вебсерверы > > (например, var/log/httpd или /var/log/apache для веб-серверов < < Апач > > на Linux) могут также регистрировать свидетельства эксплуатации.

T1190	DS0029	Содержание сетевых потоков	Используйте углубленные проверки пакетов для поиска артефактов общего режима эксплуатации, таких, как струны для впрыска SQL или известные полезные нагрузки. Например, мониторинг последовательно цепных функций, которые противники обычно злоупотребляют (т.е.
T1003	DS0026	Доступ к объекту активного каталога	] [31] [32] [33] Примечание: контроллеры домена не могут регистрировать запросы воспроизведения, исходящие из счета контроллера домена по умолчанию. [34]. Мониторинг запросов на воспроизведение [35] от IPs, не связанных с известными контроллерами домена. [21] Analytic 1 подозрительные запросы на опровержение источников_WinEventLog: Security Code="4662" и AccessMask= "0x100" и (gued= "1131f6ad 9c07 11d1 f79f 00c04fc2cd2" OR guid="1131f6a 9c07 11c04fcd2" OR guid="9923a32a 3607 11d2 b9be 000f87a36b2 OR guid"89e76 444d 4c62 991a 0facbadada6osc)]
T1003	DS0017	Выполнение команд	Монитор исполнения команд и аргументов, которые могут пытаться сбросить полномочия с помощью таких инструментов, как Mimikatz, ProcDump, NTDSUtil, или доступа к /proc, /etc/passwd, и /etc/stheow. Analytic 1 Подозрительное командное исполнение с использованием инструментов для сброса отходов. (index= Security Papers) "Invoke CachedCredentials", "Invoke LSADmp", "Invoke SAMDmDump")OR(index= Security Presource="Linux_security" IN ("Cat/et/passwed", "cat/ec/shadow", "grrep' [0 9a f] r'/proc/maps") OR(indexcamporits/ sumpact" («Инспективное сообщение»/uncifess» INS: /UnistressDAshopess/ internation» («unders/und» INDAshops/ intent/ intent/ intent/ intern» INDAshops/ IN: INDAshat/ INDS/ INDS/ IND/ IND/ IND/ INDRAshops/ int/ int/ int/ int/ IND
T1003	DS0022	Доступ к файлам	Отслеживание доступа к файлам, которые могут указывать на попытки выброса достоверных данных из различных мест хранения, таких, как LSAS память, SAM, NTDS.dit, LSA секреты, закодированные документы домена, прок файловая система, /etc/passwd, и /etc/sthenow.Analytic 1 Несанкционированный доступ к архивным файлам.
T1003	DS0022	Создание файла	Монитор неожиданного создания файлов свалки памяти для процессов, которые могут содержать полномочия. Analytic 1 Неожиданное создание свалки памяти. (index= Security survey Plaype="WinEventLog: Security: Security Code" ("Lass.dmp", "\config\SAM", "untds.dit", "\policy\secrets", "\cach"))OR (index= Security source"= "Linux_sashe" (Key="pati" значение IN ("/etc/passwd", "/etc/sheadow")) (index= source="macOS: Unified Log" сообщение IN ("(var/d/show/hashash/*), "/pervent/c/master.passwd")

T1003	DS0029	Содержание сетевых потоков	Монитор для сетевых протоколов [31] [36] и других запросов на воспроизведение [35] от IP, не связанных с известными диспетчерами доменов. [21] Analytic 1 Anomalus transport control control controls Index=Stencils = "Tream:tcp" dest_port=389 HE [открытое вводное исследование известное_dc_ip_адресы : ip] никеля SourceIP = src_ip, DestinationIP = dest_ip, протокол = Proto research (содержание = "LDAPSearch Cense") OR (содержание = "LDAPModification Cense") OR (содержание = "ind Proceeding Entry") OR (содержание = "NTDS.dit")
T1003	DS0029	Сетевой поток	Мониторинг сетевых данных для необычных потоков данных. Процессы с использованием сети, которые обычно не имеют сетевой связи или никогда ранее не были замечены, подозрительны.
T1003	DS0009	OS API Исполнение	Monitor for API звонит, который может попытаться выкинуть из операционной системы и программного обеспечения верительные грамоты, чтобы получить доступ к счетам и аттестатные материалы, как правило, в виде хеширования или четкого текстового пароля.
T1003	DS0009	Доступ к процессу	"Monitor for subsystem Service" (LSASSS) — процесс открытия процесса, поиска ключа секретов LSA и расшифровки участков в памяти, где хранятся реквизитные данные.
T1003	DS0009	Создание процессов	Монитор недавно реализованных процессов, которые могут свидетельствовать о квалификационном сбросе. Analytic 1 Неожиданное создание процесса, связанного с квалификационным сбросом. (index= Security sourcety="WinEventLog: Security Code" (4688 Image="procdum.ex" CommandLine IN ("ma lsass"))OR (index= Security Sourcy Performer="Linux_safety" (Key="cmdline" IN ("procdmap ma/proc/$(pgrep lsass")")) (Key= "exe" значение="procdum" (index= source""macOS: Unified Log" — процесс "procdum" команда" ma/proc/$(preprept lsas))
T1003	DS0024	Доступ к серверу Windows	Monitor for the SAM Creview by the SAM cystem доступ к ключу регистрации, который может попытаться выкинуть документы для получения доступа к аккаунту и аттестатного материала, как правило, в форме хеширования или четкого текстового пароля, из операционной системы и программного обеспечения. Analytic 1 Unlighted view доступ к ключу SAM. Index= Security sourcus="WinEventLog: Security" Code = 4663 ActeName"*\SAM" ¶ ¶ там, где процесс Name IN ("mimikatz.exe", "procadum.exe", "reg.exe", "reg.exe", "wmic.exe", "whall.exe", "schtasks.exe", "cmd.exe").

Таблица 6 – Меры ликвидации последствий инцидентов относительно техники

id Техники	id Меры	Название меры	Рекомендации по ликвидации последствий

T1560	M1047	Ревизия	Сканирование системы может проводиться для выявления несанкционированных архивных служб.
T1584.005	M1056	Предварительный компромисс	Этот метод не может быть легко смягчен превентивным контролем, поскольку он основан на поведении, осуществляемом вне рамок защиты и контроля предприятий.
T1189	M1048	Изоляция и сэндбоксирование	Для смягчения некоторых последствий эксплуатации можно использовать песчаные ящики, однако по-прежнему могут существовать и другие виды виртуализации и микросегментации при применении.
T1189	M1050	Защита от взрывов	Для смягчения некоторых последствий эксплуатации могут использоваться прикладные программы защиты, которые используют в процессе эксплуатации, такие, как Windows Defender Exploit Guard (WDEG) и усовершенствованный инструментарий для оценки опыта в области смягчения последствий (EMET). [70] Проверка целостности контрольного потока является еще одним способом, позволяющим потенциально определить и остановить использование программного обеспечения. [71] Многие из этих средств защиты зависят от архитектуры и двоичного приложения для целей совместимости.
T1189	M1021	Ограничение содержания на веб-сайте	В случае злонамеренного кода, подаваемого через рекламу, адблокаторы могут помочь предотвратить исполнение этого кода в первую очередь. Скрипт, блокирующий расширения, может помочь предотвратить исполнение JavaScript, который может быть обычно использован в процессе разработки.
T1189	M1051	Обновление программного обеспечения	Убедитесь, что все браузеры и подсказки, которые обновляются, могут помочь предотвратить фазу эксплуатации этого метода. Используйте современные браузеры с включёнными элементами защиты.
T1553	M1038	Профилактика исполнения	Настройка системы может предотвратить запуск приложений, которые не были загружены через Apple Store (или другие законные хранилища), что может помочь смягчить некоторые из этих проблем. Кроме того, создать возможности для решения вопросов управления приложениями, таких, как AppLocker и/или Cystem Security, чтобы блокировать загрузку злонамеренного контента.
T1553	M1028	Конфигурация операционной системы	Windows Group Policy можно использовать для управления корневыми сертификатами, а значение флагов HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\Root_ProtectedRoots может быть установлено на 1, чтобы не дать пользователям, не являющимся администраторами, возможность создавать дополнительные корневые установки в своем собственном магазине сертификатов HKCU. [5]
T1553	M1026	Привилегированное управление счетами	Управление созданием, модификацией, использованием и разрешениями, связанными с привилегированными счетами, включая систему и корневое происхождение.
T1553	M1024	Ограничить полномочия регистра	Обеспечение наличия надлежащих разрешений для регистрационных ульев, с тем чтобы не допустить изменения пользователями ключей, связанных с SIP и компонентами доверительных поставщиков.

T1553	M1054	Конфигурация программного обеспечения	HTTP Public Key Pinning (HPKP) является одним из методов смягчения потенциальных проблем в ситуациях на Ближнем Востоке, когда и противник использует неправильно выданный или поддельный сертификат для перехвата зашифрованных сообщений путем принудительного использования ожидаемого сертификата. [6]
T1021.001	M1047	Ревизия	Регулярно проверять членский состав группы пользователей дистанционных настольных компьютеров. Удалять ненужные счета и группы из групп пользователей дистанционных настольных компьютеров.
T1021.001	M1042	Отключить или удалить функцию или программу	Отключить сервис RDP, если в этом нет необходимости.
T1021.001	M1035	Ограничение доступа к сети ресурсов	Используйте дистанционные настольные врата.
T1021.001	M1032	Многофакторная аутентификация	Использовать многофакторную аутентификацию для удаленных входов[76].
T1021.001	M1030	Сегмент сети	Не оставляйте доступ к RDP из Интернета. Предоставьте правила брандмауэра для блокировки трафика RDP между сетевыми зонами безопасности в сети.
T1021.001	M1028	Конфигурация операционной системы	Изменить GPO, с тем чтобы определить более короткие продолжительные сеансы и максимальное количество времени, которое может быть задействовано в любой отдельной сессии.
T1021.001	M1026	Привилегированное управление счетами	Рассмотреть вопрос об исключении группы местных администраторов из списка групп, которым разрешено зарегистрироваться через ПДР.
T1021.001	M1018	Управление счетами пользователей	Ограничить дистанционное разрешение пользователя, если необходим дистанционный доступ.
T1583.002	M1056	Предварительный компромисс	Этот метод не может быть легко смягчен превентивным контролем, поскольку он основан на поведении, осуществляемом вне рамок защиты и контроля предприятий.
T1566	M1049	Антивирус/противомалярийное средство	Антивирус может автоматически карантинировать подозрительные файлы.

T1566	M1047	Ревизия	Проводить проверки или сканирование систем, разрешений, ненадежного программного обеспечения, ненадежных конфигураций и т.д. для выявления потенциальных недостатков.
T1566	M1031	Профилактика вмешательства в сеть	Для блокирования деятельности могут использоваться системы и системы предупреждения проникновения в сеть, предназначенные для сканирования и удаления злонамеренных вложений или ссылок по электронной почте.
T1566	M1021	Ограничение содержания на веб-сайте	), которые могут быть использованы для фишинга, необходимы для деловых операций, и рассмотреть вопрос о блокировании доступа, если деятельность не поддается тщательному мониторингу или если она сопряжена со значительным риском.
T1566	M1054	Конфигурация программного обеспечения	Использование механизмов аутентификации сообщений против спуфинга и электронной почты для фильтрации сообщений на основе проверки действительности домена отправителя (с использованием SPF) и целостности сообщений (с использованием DKIM).
T1566	M1017	Обучение пользователей	Пользователи могут быть обучены методам социальной инженерии и фишинг-мейлы.
T1190	M1048	Изоляция и сэндбоксирование	Изоляция применения ограничит доступ к другим процессам и системе, к которым может иметь доступ эксплуатируемый объект.
T1190	M1050	Защита от взрывов	Для ограничения воздействия прикладных программ, с тем чтобы предотвратить попадание прикладных программ в приложение для эксплуатации транспортных средств, могут использоваться брандмауэры Web-приложений.
T1190	M1030	Сегмент сети	Сегмент внешних серверов и услуг из остальной части сети с ДМЗ или на отдельной хостинговой инфраструктуре.
T1190	M1026	Привилегированное управление счетами	Использование наименьших привилегий для счетов услуг ограничит то, какие разрешения получает эксплуатируемый процесс на остальной части системы.
T1190	M1051	Обновление программного обеспечения	Регулярное обновление программного обеспечения путем использования системы патч для внешних прикладных программ.
T1190	M1016	Сканирование уязвимости	Регулярное сканирование внешних систем на предмет выявления факторов уязвимости и установление процедур быстрого изменения систем в тех случаях, когда в результате сканирования и обнародования информации выявляются важнейшие факторы уязвимости[8].
T1003	M1015	Активная конфигурация каталога	Управление контрольным списком доступа для "Replication Directory All" и других разрешений, связанных с воспроизведением домена контроллеров. [21] [22] Рассмотреть вопрос о добавлении пользователей в группу защиты активного каталога "Protected Users". Это может помочь ограничить клетку текстовых данных пользователей[23].

T1003	M1040	Профилактика поведения в конечном итоге	На " Windows 10 " можно использовать правила, касающиеся сокращения поверхности атаки (ACP), для обеспечения безопасности СУСАС и предотвращения кражи документов. [24]
T1003	M1043	Защита конфиденциального доступа	С Windows 10 Microsoft внедрила новые средства защиты под названием Credential Guardy для защиты секретов LSA, которые могут быть использованы для получения документов с помощью форм аттестатного демпинга.
T1003	M1041	Зашифровать чувствительную информацию	Обеспечивать надлежащее обеспечение резервного копирования домена.
T1003	M1028	Конфигурация операционной системы	Рассмотреть вопрос об утрате или ограничении NTLM[27] Рассмотреть вопрос об аннулировании WDigest аутентификации[28].
T1003	M1027	Политика пароля	Обеспечить наличие сложных и уникальных паролей на счетах местных администраторов во всех системах сети.
T1003	M1026	Привилегированное управление счетами	Windows: Не помещайте пользовательские или администрированные донные счета в местные группы администраторов через системы, если только они не строго не контролируются, поскольку это часто эквивалентно тому, что у местного администратора есть один и тот же пароль на всех системах. Следовать наилучшей практике проектирования и управления корпоративной сетью для ограничения использования привилегированных счетов на всех административных уровнях. [29] Linux:Scrafting пароли из памяти требуют основополагающих привилегий. Следовать наилучшей практике ограничения доступа к привилегированным счетам во избежание враждебных программ от доступа к таким чувствительным регионам памяти.
T1003	M1025	Привилегированная добросовестность процесса	На Windows 8.1 и Windows Server 2012 R2 можно использовать защищенный процесс Light для LSA[30].
T1003	M1017	Обучение пользователей	Ограничение совпадения данных между счетами и системами путем обучения пользователей и администраторов не использовать один и тот же пароль для нескольких счетов.

Таблица 7 – Функциональные знания и умения

id Должности	Должность ИБ	id Техники	Компетенции сотрудника ИБ

E1	Системный администратор	T1189	Управление доступами пользователей, Обеспечение безопасности веб-приложений, Управление учетными записями пользователей, Управление безопасностью приложений, Поддержка пользователей и консультирование, Анализ поведения пользователей и обнаружение аномалий, Управление правами доступа к файловым системам, Управление системой контроля версий, Управление системой управления идентификацией и доступом (IAM), Разработка скриптов автоматизации
E1	Системный администратор	T1553	Управление сертификатами безопасности, Поддержка пользователей и консультирование, Управление доступами пользователей, Управление учетными записями пользователей, Знание операционных систем Windows/Linux/MacOS, Управление системой контроля версий, Управление правами доступа к файловым системам, Мониторинг и управление системами безопасности, Анализ поведения пользователей и обнаружение аномалий, Настройка систем мониторинга событий безопасности
E1	Системный администратор	T1021.001	Настройка удаленного доступа, Управление доступами пользователей, Работа с облачными сервисами, Управление учетными записями пользователей, Взаимодействие с внешними поставщиками услуг, Управление правами доступа к файловым системам, Управление системой управления идентификацией и доступом (IAM), Настройка систем видеонаблюдения и контроля доступа, Знание операционных систем Windows/Linux/MacOS, Поддержка пользователей и консультирование
E1	Системный администратор	T1566	Защита от внешних угроз (DDoS, фишинг), Знание методов социальной инженерии, Контроль за соблюдением правил использования электронной почты, Настройка удаленного доступа, Управление учетными записями пользователей, Управление правами доступа к файловым системам, Управление доступами пользователей, Управление системой управления идентификацией и доступом (IAM), Мониторинг и управление системами безопасности, Работа с системами управления конфигурациями
E1	Системный администратор	T1584.005	Работа с облачными сервисами, Защита от внешних угроз (DDoS, фишинг), Взаимодействие с внешними поставщиками услуг, Работа с системами управления конфигурациями, Настройка сетевого оборудования, Мониторинг и управление системами безопасности, Оптимизация производительности систем, Работа с системами мониторинга производительности, Управление системой контроля версий, Настройка систем мониторинга событий безопасности
E1	Системный администратор	T1560	Шифрование данных, Резервное копирование данных, Разработка планов миграции данных, Управление политиками шифрования, Разработка сценариев восстановления данных, Обеспечение конфиденциальности персональных данных, Анализ и обработка больших объемов данных, Контроль за соблюдением правил хранения данных, Работа с системами предотвращения утечек данных (DLP), Управление жизненным циклом ключей шифрования

E1	Системный администратор	T1190	Управление системой управления идентификацией и доступом (IAM), Управление доступами пользователей, Управление правами доступа к файловым системам, Разработка политик использования мобильных устройств, Настройка сетевого оборудования, Управление безопасностью приложений, Управление рисками при использовании мобильных устройств, Работа с облачными сервисами, Умение работать с базами данных, Управление правами доступа к ресурсам
E1	Системный администратор	T1583.002	Администрирование серверных платформ, Настройка и обслуживание почтовых серверов, Управление системой контроля версий, Управление безопасностью приложений, Настройка систем видеонаблюдения и контроля доступа, Обеспечение безопасности веб-приложений, Разработка инструкций по эксплуатации систем, Поддержка пользователей и консультирование, Автоматизация рутинных задач, Управление системой управления инцидентами (IRM)
E1	Системный администратор	T1003	Использование средств анализа уязвимостей, Управление учетными записями пользователей, Управление паролями и аутентификацией, Проведение тренингов по защите информации, Реагирование на инциденты информационной безопасности, Оценка рисков информационной безопасности, Консультирование по вопросам информационной безопасности, Управление доступами пользователей, Работа с системами управления событиями безопасности (SIEM), Настройка удаленного доступа
E2	Архитектор ИБ	T1189	Опыт работы с системами безопасности веб-приложений, Опыт работы с системами управления доступом (IAM), Опыт разработки архитектуры безопасности для различных типов приложений, Знание уязвимостей и способов их эксплуатации, Опыт работы с системами защиты от Brute-force атак, Опыт работы с системами защиты от Clickjacking-атак, Опыт работы с системами защиты от CSRF-атак, Опыт работы с системами защиты от XSS-атак, Опыт работы с системами защиты от DDoS-атак, Опыт работы с системами защиты от вредоносного ПО
E2	Архитектор ИБ	T1553	Опыт работы с системами управления цифровыми сертификатами, Опыт работы с системами мониторинга безопасности, Опыт работы с системами безопасности почты, Опыт работы с системами безопасности для IoT-устройств, Знание различных методов шифрования, Знание уязвимостей и способов их эксплуатации, Опыт работы с системами безопасности веб-приложений, Опыт работы с системами безопасности для промышленной автоматизации, Опыт работы с системами безопасности для мобильных устройств, Опыт работы с системами анализа больших данных и их безопасности
E2	Архитектор ИБ	T1021.001	Опыт работы с системами управления доступом (IAM), Опыт работы с криптографическими протоколами, Опыт работы с системами защиты от вредоносного ПО, Опыт работы с системами SIEM, Опыт работы с системами фаерволов, Опыт работы с системами безопасности для IoT-устройств, Опыт работы с системами мониторинга безопасности, Опыт работы с системами безопасности почты, Опыт проектирования защищенных систем, Опыт работы с системами управления рисками

E2	Архитектор ИБ	T1566	Опыт работы с системами безопасности почты, Опыт работы с системами управления доступом (IAM), Опыт работы с системами мониторинга безопасности, Опыт работы с системами управления рисками, Опыт работы с системами управления событиями безопасности (SEM), Опыт работы с системами защиты от вредоносного ПО, Опыт работы с системами управления цифровыми сертификатами, Опыт работы с методологиями разработки безопасного ПО (SDL), Знание методологий оценки рисков (например, FAIR), Опыт работы с системами безопасности для IoT-устройств
E2	Архитектор ИБ	T1584.005	Опыт работы с системами защиты от DDoS-атак, Опыт работы с VPN-сетями, Понимание принципов построения защищенных сетей, Опыт работы с системами фаерволов, Опыт работы с системами SIEM, Опыт работы с системами безопасности почты, Опыт работы с системами безопасности для IoT-устройств, Опыт работы с системами мониторинга безопасности, Опыт работы с системами управления рисками, Опыт проектирования защищенных систем
E2	Архитектор ИБ	T1560	Опыт работы с системами резервного копирования и восстановления данных, Опыт работы с системами анализа больших данных и их безопасности, Знание различных методов шифрования, Опыт работы с системами защиты от утечки информации (DLP), Понимание угроз безопасности информации, Опыт разработки и внедрения систем обнаружения вторжений (IDS/IPS), Знание уязвимостей и способов их эксплуатации, Знание стандартов безопасности информации (ISO 27001, NIST, PCI DSS и др.), Опыт работы с системами управления событиями безопасности (SEM), Опыт работы с системами защиты от вредоносного ПО
E2	Архитектор ИБ	T1190	Опыт работы с системами управления доступом (IAM), Опыт работы с системами безопасности для мобильных устройств, Опыт работы с VPN-сетями, Понимание принципов построения защищенных сетей, Опыт работы с системами управления ключами (PKI), Опыт работы с системами безопасности веб-приложений, Опыт работы с облачными технологиями и их безопасностью, Опыт работы с системами управления рисками, Опыт работы с различными типами баз данных и их защиты, Знание уязвимостей и способов их эксплуатации
E2	Архитектор ИБ	T1583.002	Опыт работы с системами безопасности веб-приложений, Опыт разработки архитектуры безопасности для различных типов приложений, Опыт работы с системами защиты от вредоносного ПО, Опыт работы с различными типами баз данных и их защиты, Знание различных методов шифрования, Опыт работы с системами SIEM, Опыт работы с системами фаерволов, Опыт работы с системами безопасности для IoT-устройств, Опыт работы с системами мониторинга безопасности, Опыт работы с системами безопасности почты
E2	Архитектор ИБ	T1003	Понимание угроз безопасности информации, Опыт работы с системами управления доступом (IAM), Знание стандартов безопасности информации (ISO 27001, NIST, PCI DSS и др.), Опыт работы с системами мониторинга безопасности, Опыт работы с системами безопасности почты, Опыт работы с системами безопасности для IoT-устройств, Опыт работы с микросервисной архитектурой и её защитой, Опыт разработки политик безопасности, Знание архитектурных принципов безопасности, Опыт работы с системами безопасности веб-приложений

E3	Аналитик ИБ	T1189	Анализ атак на веб-приложения, Анализ вредоносного кода, Выявление аномалий в активности пользователей, Опыт работы с системами управления доступом, Написание скриптов для анализа данных, Опыт работы с системами защиты от вредоносного ПО, Опыт работы с системами защиты от DDoS-атак, Опыт работы с системами мониторинга безопасности, Опыт работы с системами управления уязвимостями, Опыт работы с системами управления рисками
E3	Аналитик ИБ	T1553	Выявление аномалий в активности пользователей, Анализ вредоносного кода, Форензика (Digital Forensics), Анализ цифровых следов, Опыт работы с системами мониторинга безопасности, Настройка и поддержка систем безопасности, Знание операционных систем (Windows, Linux, macOS), Анализ логов безопасности, Анализ событий безопасности, Корреляция данных безопасности
E3	Аналитик ИБ	T1021.001	Опыт работы с системами управления доступом, Анализ логов безопасности, Выявление аномалий в активности пользователей, Опыт работы с системами защиты от вредоносного ПО, Знание операционных систем (Windows, Linux, macOS), Опыт работы с системами мониторинга безопасности, Использование систем SIEM (Splunk, QRadar, ArcSight), Опыт работы с системами управления рисками, Опыт работы с системами управления уязвимостями, Опыт работы с системами защиты от DDoS-атак
E3	Аналитик ИБ	T1566	Анализ фишинговых атак, Анализ вредоносного кода, Опыт работы с системами управления доступом, Опыт работы с системами мониторинга безопасности, Обратная разработка (Reverse Engineering), Опыт работы с системами управления рисками, Опыт работы с системами управления уязвимостями, Опыт работы с системами защиты от вредоносного ПО, Анализ вредоносного ПО (Malware Analysis), Настройка и поддержка систем безопасности
E3	Аналитик ИБ	T1584.005	Опыт работы с системами защиты от DDoS-атак, Выявление аномалий в активности пользователей, Анализ сетевых атак, Опыт работы с системами мониторинга безопасности, Опыт работы с системами защиты от вредоносного ПО, Опыт работы с системами управления рисками, Опыт работы с системами управления уязвимостями, Опыт работы с системами управления доступом, Анализ сетевого трафика, Опыт работы с системами аутентификации и авторизации
E3	Аналитик ИБ	T1560	Визуализация данных, Восстановление данных, Корреляция данных безопасности, Написание скриптов для анализа данных, Анализ данных из различных источников, Опыт работы с системами защиты от утечки информации (DLP), Выявление аномалий в сетевом трафике, Выявление аномалий в активности пользователей, Знание стандартов безопасности информации (ISO 27001, NIST, PCI DSS), Использование систем анализа угроз (Threat Intelligence Platforms)
E3	Аналитик ИБ	T1190	Опыт работы с системами управления доступом, Знание принципов работы сетевых устройств (роутеры, свитчи), Анализ сетевых атак, Анализ атак на IoT-устройства, Анализ атак на мобильные устройства, Анализ сетевого трафика, Опыт работы с системами управления рисками, Опыт работы с системами управления уязвимостями, Идентификация сетевых атак, Работа с базами данных (SQL, NoSQL)

E3	Аналитик ИБ	T1583.002	Знание протоколов сетевой безопасности (TCP/IP, HTTP, HTTPS, DNS), Анализ атак на веб-приложения, Анализ сетевого трафика, Выявление аномалий в сетевом трафике, Расследование инцидентов безопасности (Incident Response), Работа с инструментами анализа трафика (Wireshark, tcpdump), Анализ вредоносного ПО (Malware Analysis), Опыт работы с системами защиты от вредоносного ПО, Анализ данных из различных источников, Знание принципов работы систем безопасности (фаерволы, IDS/IPS)
E3	Аналитик ИБ	T1003	Работа с инструментами анализа памяти (Volatility), Работа с инструментами анализа трафика (Wireshark, tcpdump), Опыт работы с системами управления доступом, Использование инструментов для пентестинга (Metasploit, Nmap), Знание стандартов безопасности информации (ISO 27001, NIST, PCI DSS), Анализ логов безопасности, Анализ событий безопасности, Корреляция данных безопасности, Опыт работы с системами мониторинга безопасности, Опыт работы с облачными технологиями и их безопасностью
E4	Тестировщик проникновения	T1189	Опыт проведения различных типов пентестов (веб-приложений, сетей, мобильных приложений, API), Написание эксплойтов, Опыт работы с инструментами для анализа веб-приложений (Burp Suite, ZAP, OWASP Juice Shop), Опыт работы с системами управления доступом (IAM) (AWS IAM, Azure AD, Okta), Опыт работы с инструментами для анализа мобильных приложений (MobSF, Drozer), Опыт работы с системами защиты от DDoS-атак (mitigation techniques), Опыт использования различных техник обхода систем безопасности (bypass techniques), Опыт работы с системами защиты от вредоносного ПО (обход антивирусных систем), Разработка и использование собственных инструментов для пентестинга (скрипты, фреймворки), Опыт анализа логов безопасности (анализ логов веб-серверов, баз данных, системных логов)
E4	Тестировщик проникновения	T1553	Опыт работы с системами управления ключами (PKI) (SSL/TLS сертификаты), Опыт использования различных техник обхода систем безопасности (bypass techniques), Опыт работы с системами аутентификации и авторизации (Kerberos, OAuth 2.0, OpenID Connect), Знание операционных систем (Windows, Linux, macOS, Android, iOS), Опыт работы с системами мониторинга безопасности (SIEM) (Splunk, QRadar, ELK stack), Опыт работы с облачными технологиями и их безопасностью (AWS, Azure, GCP), Опыт работы с базами данных и их безопасностью (SQL, NoSQL, MongoDB, PostgreSQL), Опыт работы с контейнеризацией и оркестрацией (Docker, Kubernetes, безопасность контейнеров), Опыт работы с инструментами для анализа бинарных файлов (IDA Pro, Ghidra, objdump), Знание уязвимостей и способов их эксплуатации (OWASP Top 10, SANS Top 25)

E4	Тестировщик проникновения	T1021.001	Опыт анализа логов безопасности (анализ логов веб-серверов, баз данных, системных логов), Опыт работы с системами защиты от вредоносного ПО (обход антивирусных систем), Опыт работы с системами управления доступом (IAM) (AWS IAM, Azure AD, Okta), Опыт использования различных техник обхода систем безопасности (bypass techniques), Опыт работы с системами защиты от DDoS-атак (mitigation techniques), Опыт работы с системами аутентификации и авторизации (Kerberos, OAuth 2.0, OpenID Connect), Знание операционных систем (Windows, Linux, macOS, Android, iOS), Опыт работы с системами обнаружения вторжений (IDS/IPS) и их обхода (evasion techniques), Опыт работы с системами защиты от утечки информации (DLP) (обход DLP-систем), Опыт анализа сетевого трафика (глубокий анализ пакетов, протокольный анализ)
E4	Тестировщик проникновения	T1566	Опыт использования различных техник обхода систем безопасности (bypass techniques), Опыт работы с системами управления доступом (IAM) (AWS IAM, Azure AD, Okta), Опыт работы с системами защиты от вредоносного ПО (обход антивирусных систем), Опыт работы с системами управления ключами (PKI) (SSL/TLS сертификаты), Опыт работы с системами защиты от DDoS-атак (mitigation techniques), Опыт работы с системами обнаружения вторжений (IDS/IPS) и их обхода (evasion techniques), Опыт работы с системами мониторинга безопасности (SIEM) (Splunk, QRadar, ELK stack), Опыт работы с системами аутентификации и авторизации (Kerberos, OAuth 2.0, OpenID Connect), Опыт работы с инструментами для анализа бинарных файлов (IDA Pro, Ghidra, objdump), Опыт работы с фаерволами и их обхода (прокси, VPN, туннелирование)
E4	Тестировщик проникновения	T1584.005	Опыт работы с системами защиты от DDoS-атак (mitigation techniques), Опыт работы с системами защиты от вредоносного ПО (обход антивирусных систем), Опыт работы с системами защиты от утечки информации (DLP) (обход DLP-систем), Опыт анализа сетевого трафика (глубокий анализ пакетов, протокольный анализ), Опыт работы с системами предотвращения вторжений (IPS) и их обхода, Опыт проведения различных типов пентестов (веб-приложений, сетей, мобильных приложений, API), Опыт работы с системами обнаружения вторжений (IDS/IPS) и их обхода (evasion techniques), Опыт работы с системами управления ключами (PKI) (SSL/TLS сертификаты), Опыт использования различных техник обхода систем безопасности (bypass techniques), Опыт работы с системами аутентификации и авторизации (Kerberos, OAuth 2.0, OpenID Connect)
E4	Тестировщик проникновения	T1560	Опыт работы с системами защиты от утечки информации (DLP) (обход DLP-систем), Разработка и использование собственных инструментов для пентестинга (скрипты, фреймворки), Опыт анализа сетевого трафика (глубокий анализ пакетов, протокольный анализ), Знание уязвимостей и способов их эксплуатации (OWASP Top 10, SANS Top 25), Знание методологий оценки рисков (FAIR, OCTAVE, STRIDE), Опыт работы с системами предотвращения вторжений (IPS) и их обхода, Опыт работы с системами защиты от DDoS-атак (mitigation techniques), Опыт работы с системами управления ключами (PKI) (SSL/TLS сертификаты), Опыт работы с системами управления доступом (IAM) (AWS IAM, Azure AD, Okta), Опыт работы с системами аутентификации и авторизации (Kerberos, OAuth 2.0, OpenID Connect)

E4	Тестировщик проникновения	T1190	Знание уязвимостей и способов их эксплуатации (OWASP Top 10, SANS Top 25), Написание эксплойтов, Опыт работы с системами управления доступом (IAM) (AWS IAM, Azure AD, Okta), Опыт проведения различных типов пентестов (веб-приложений, сетей, мобильных приложений, API), Опыт анализа сетевого трафика (глубокий анализ пакетов, протокольный анализ), Опыт работы с контейнеризацией и оркестрацией (Docker, Kubernetes, безопасность контейнеров), Опыт работы с системами управления ключами (PKI) (SSL/TLS сертификаты), Опыт работы с базами данных и их безопасностью (SQL, NoSQL, MongoDB, PostgreSQL), Опыт работы с инструментами для анализа веб-приложений (Burp Suite, ZAP, OWASP Juice Shop), Опыт работы с облачными технологиями и их безопасностью (AWS, Azure, GCP)
E4	Тестировщик проникновения	T1583.002	Понимание принципов работы различных протоколов (TCP/IP, HTTP, HTTPS, DNS, SMTP, IMAP, POP3, FTP, SSH), Опыт анализа логов безопасности (анализ логов веб-серверов, баз данных, системных логов), Опыт проведения различных типов пентестов (веб-приложений, сетей, мобильных приложений, API), Опыт анализа сетевого трафика (глубокий анализ пакетов, протокольный анализ), Опыт работы с системами защиты от вредоносного ПО (обход антивирусных систем), Опыт работы с инструментами для анализа мобильных приложений (MobSF, Drozer), Опыт работы с инструментами для анализа веб-приложений (Burp Suite, ZAP, OWASP Juice Shop), Опыт использования различных техник обхода систем безопасности (bypass techniques), Понимание принципов работы различных технологий (websockets, REST API, GraphQL), Опыт работы с системами защиты от утечки информации (DLP) (обход DLP-систем)
E4	Тестировщик проникновения	T1003	Опыт работы с инструментами для анализа памяти (Volatility, Rekall), Разработка и использование собственных инструментов для пентестинга (скрипты, фреймворки), Опыт работы с fuzzing-инструментами (Radamsa, boofuzz), Опыт работы с инструментами для анализа мобильных приложений (MobSF, Drozer), Опыт написания отчетов о результатах пентеста (четкое и понятное описание уязвимостей и рекомендаций), Опыт работы с инструментами для анализа бинарных файлов (IDA Pro, Ghidra, objdump), Опыт работы с системами управления доступом (IAM) (AWS IAM, Azure AD, Okta), Опыт работы с инструментами для анализа веб-приложений (Burp Suite, ZAP, OWASP Juice Shop), Опыт работы с инструментами для пентестинга (Metasploit, Nmap, Burp Suite, Wireshark, sqlmap, Nikto), Опыт работы с облачными технологиями и их безопасностью (AWS, Azure, GCP)
E5	Инженер по безопасности	T1189	Опыт работы с системами безопасности веб-приложений (WAF), Опыт работы с системами безопасности веб-приложений (OWASP Top 10), Опыт работы с технологиями безопасности приложений (Application Security), Установка и настройка систем управления доступом (IAM), Опыт работы с системами безопасности мобильных приложений (MAM), Опыт работы с системами безопасности веб-приложений (WAF) - Cloudflare WAF, AWS WAF, ModSecurity, Опыт работы с системами безопасности мобильных приложений (MAM) - MobileIron, VMware Workspace ONE, Установка и настройка систем управления доступом (IAM) - Azure AD, AWS IAM, Okta, Ping Identity, Написание скриптов для автоматизации задач безопасности, Опыт работы с системами защиты от Brute-force атак

E5	Инженер по безопасности	T1553	Опыт работы с системами управления цифровыми сертификатами, Понимание принципов zero trust security, Опыт работы с системами управления цифровыми сертификатами (Let's Encrypt, DigiCert, Entrust, создание и управление сертификатами), Опыт работы с системами безопасности промышленной автоматизации (ICS/SCADA) (безопасность SCADA-систем), Опыт работы с системами безопасности промышленной автоматизации (ICS/SCADA), Опыт работы с различными методами анализа безопасности, Знание операционных систем (Windows, Linux, macOS), Опыт работы с системами автоматизации безопасности (Security Automation), Опыт работы с различными методами тестирования, Знание различных методов шифрования
E5	Инженер по безопасности	T1021.001	Установка и настройка систем управления доступом (IAM), Опыт работы с микросервисной архитектурой и её защитой (API Gateway, Service Mesh), Опыт работы с облачными технологиями и их безопасностью (AWS, Azure, GCP, безопасность облачных сервисов), Установка и настройка систем управления доступом (IAM) - Azure AD, AWS IAM, Okta, Ping Identity, Опыт работы с системами анализа больших данных и их безопасности (Splunk, Elastic Stack, анализ логов, машинное обучение), Установка и настройка систем защиты от вредоносного ПО (EDR), Знание операционных систем (Windows, Linux, macOS), Опыт работы с криптографическими протоколами (TLS, SSH, IPsec), Опыт работы с системами автоматизации (Jenkins, GitLab CI, GitHub Actions), Опыт работы с криптографическими протоколами (TLS, SSH, IPsec, PGP)
E5	Инженер по безопасности	T1566	Опыт работы с системами безопасности почты (SPF, DKIM, DMARC), Установка и настройка систем управления доступом (IAM), Опыт работы с различными инструментами для управления безопасностью, Настройка и мониторинг систем безопасности, Установка и настройка систем управления доступом (IAM) - Azure AD, AWS IAM, Okta, Ping Identity, Опыт работы с системами управления событиями и журналами (SIEM), Опыт работы с системами управления цифровыми сертификатами, Опыт работы с системами мониторинга производительности, Опыт работы с системами безопасности мобильных приложений (MAM), Установка и настройка систем защиты от вредоносного ПО (EDR)
E5	Инженер по безопасности	T1584.005	Установка и настройка систем защиты от DDoS-атак, Установка и настройка систем защиты от DDoS-атак - Cloudflare, Akamai, Arbor Networks, Опыт работы с микросервисной архитектурой и её защитой (API Gateway, Service Mesh), Опыт работы с облачными технологиями и их безопасностью (AWS, Azure, GCP, безопасность облачных сервисов), Опыт работы с технологиями безопасности сети (Network Security), Опыт работы с микросегментацией сети, Настройка и администрирование сетевых устройств (роутеры, свитчи), Опыт работы с системами автоматизации безопасности (Security Automation), Опыт работы с различными типами сетевых устройств (роутеры, свитчи, фаерволы), Опыт работы с системами безопасности промышленной автоматизации (ICS/SCADA) (безопасность SCADA-систем)

E5	Инженер по безопасности	T1560	Знание различных методов шифрования, Опыт работы с системами резервного копирования и восстановления данных, Опыт работы с инструментами для анализа больших данных, Опыт работы с технологиями защиты от утечек данных (Data Loss Prevention - DLP), Установка и настройка систем защиты от утечки информации (DLP), Установка и настройка систем защиты от утечки информации (DLP) - Forcepoint, McAfee DLP, Data Loss Prevention, Знание различных методов шифрования (симметричное, асимметричное, хэширование), Опыт работы с системами анализа больших данных и их безопасности (Splunk, Elastic Stack), Опыт работы с системами резервного копирования и восстановления данных (Veeam, Backup Exec, ZFS), Опыт работы с системами анализа больших данных и их безопасности (Splunk, Elastic Stack, анализ логов, машинное обучение)
E5	Инженер по безопасности	T1190	Опыт работы с системами безопасности веб-приложений (OWASP Top 10), Настройка и администрирование сетевых устройств (роутеры, свитчи), Установка и настройка систем управления доступом (IAM), Настройка и администрирование сетевых устройств (роутеры, свитчи, маршрутизаторы, балансировщики нагрузки), Опыт работы с различными типами сетевых устройств (роутеры, свитчи, фаерволы), Опыт работы с технологиями безопасности сети (Network Security), Установка и настройка систем управления доступом (IAM) - Azure AD, AWS IAM, Okta, Ping Identity, Администрирование баз данных и их защита (SQL Server, MySQL, PostgreSQL, MongoDB, безопасность баз данных), Опыт работы с микросегментацией сети, Администрирование баз данных и их защита
E5	Инженер по безопасности	T1583.002	Установка и настройка VPN-серверов, Опыт работы с различными типами протоколов (TCP/IP, HTTP, HTTPS, DNS, SMTP, FTP, SSH), Знание протоколов сетевой безопасности (TCP/IP, HTTP, HTTPS, DNS, SMTP, FTP, SSH), Знание протоколов сетевой безопасности (TCP/IP, HTTP, HTTPS, DNS, SMTP, FTP, SSH, TLS, IPsec, BGP), Установка и настройка VPN-серверов - OpenVPN, WireGuard, IPsec, Опыт работы с системами безопасности промышленной автоматизации (ICS/SCADA), Администрирование баз данных и их защита (SQL Server, MySQL, PostgreSQL, MongoDB, безопасность баз данных), Опыт работы с системами безопасности промышленной автоматизации (ICS/SCADA) (безопасность SCADA-систем), Опыт работы с технологиями безопасности приложений (Application Security), Опыт работы с системами безопасности мобильных приложений (MAM)
E5	Инженер по безопасности	T1003	Опыт работы с различными инструментами для управления безопасностью, Опыт работы с инструментами для анализа больших данных, Опыт работы с инструментами для анализа уязвимостей (Nessus, OpenVAS), Опыт работы с инструментами для анализа уязвимостей (Nessus, OpenVAS, QualysGuard, Acunetix), Опыт работы с системами управления событиями и журналами (SIEM), Установка и настройка систем управления доступом (IAM), Знание стандартов безопасности информации (ISO 27001, NIST, PCI DSS, GDPR), Знание стандартов безопасности информации (ISO 27001, NIST Cybersecurity Framework, PCI DSS, GDPR, HIPAA), Установка и настройка систем управления доступом (IAM) - Azure AD, AWS IAM, Okta, Ping Identity, Опыт работы с безопасностью баз данных (Database Security)

E6	Консультант по безопасности	T1189	Опыт работы с системами безопасности веб-приложений (WAF), Опыт работы с различными типами приложений (веб, мобильные, десктопные), Опыт работы с технологиями безопасности приложений (Application Security), Опыт работы с системами управления доступом (IAM), Опыт работы с системами безопасности мобильных приложений (MAM), Опыт разработки и внедрения систем управления доступом (IAM), Опыт работы с различными отраслями и их спецификой в области безопасности, Опыт работы с системами защиты от DDoS-атак, Опыт работы с системами защиты от вредоносного ПО, Опыт работы с системами управления информационной безопасностью (ISMS)
E6	Консультант по безопасности	T1553	Опыт работы с системами управления цифровыми сертификатами, Понимание принципов zero trust security, Разработка и внедрение программ обеспечения безопасности, Опыт разработки и внедрения программ обучения персонала по информационной безопасности, Понимание принципов архитектуры безопасности (микросегментация, Zero Trust), Опыт работы с различными методами анализа безопасности, Опыт работы с различными отраслями и их спецификой в области безопасности, Знание операционных систем (Windows, Linux, macOS), Опыт работы с различными методами тестирования, Опыт работы с системами автоматизации безопасности (Security Automation)
E6	Консультант по безопасности	T1021.001	Опыт работы с различными типами приложений (веб, мобильные, десктопные), Опыт работы с системами управления доступом (IAM), Опыт разработки и внедрения систем управления доступом (IAM), Опыт работы с системами управления событиями и журналами (SIEM), Опыт работы с системами защиты от вредоносного ПО, Знание операционных систем (Windows, Linux, macOS), Опыт работы с криптографическими протоколами (TLS, SSH, IPsec), Опыт работы с системами автоматизации безопасности (Security Automation), Опыт работы с системами управления рисками, Опыт работы с системами управления уязвимостями
E6	Консультант по безопасности	T1566	Опыт работы с системами управления доступом (IAM), Опыт разработки и внедрения систем управления доступом (IAM), Опыт работы с различными отраслями и их спецификой в области безопасности, Опыт работы с системами управления рисками, Опыт работы с системами управления уязвимостями, Опыт работы с системами защиты от вредоносного ПО, Опыт работы с системами управления информационной безопасностью (ISMS), Опыт работы с системами мониторинга безопасности (SIEM), Опыт работы с системами управления цифровыми сертификатами, Опыт работы с системами управления событиями и журналами (SIEM)
E6	Консультант по безопасности	T1584.005	Опыт работы с системами защиты от DDoS-атак, Опыт работы с технологиями безопасности сети (Network Security), Опыт работы с микросегментацией сети, Опыт работы с системами автоматизации безопасности (Security Automation), Опыт работы с системами управления рисками, Опыт работы с системами управления уязвимостями, Опыт работы с системами безопасности IoT-устройств, Опыт работы с системами анализа безопасности (Security Analytics), Опыт работы с системами защиты от вредоносного ПО, Опыт работы с системами аутентификации и авторизации

E6	Консультант по безопасности	T1560	Знание различных методов шифрования, Опыт работы с системами анализа больших данных и их безопасности, Опыт работы с системами защиты от утечки информации (DLP), Опыт работы с технологиями защиты от утечек данных (Data Loss Prevention - DLP), Консультирование по вопросам защиты данных (GDPR, CCPA), Опыт работы с различными методами анализа безопасности, Опыт работы с различными методами тестирования, Опыт работы с различными методами тестирования на проникновение, Опыт работы с системами обнаружения вторжений (IDS/IPS), Разработка политик безопасности информации
E6	Консультант по безопасности	T1190	Опыт работы с системами управления доступом (IAM), Опыт разработки и внедрения систем управления доступом (IAM), Опыт работы с технологиями безопасности сети (Network Security), Опыт работы с микросегментацией сети, Опыт работы с технологиями безопасности контейнеров (AppArmor, SELinux), Опыт работы с безопасностью баз данных (Database Security), Опыт работы с базами данных и их безопасностью, Знание протоколов сетевой безопасности (TCP/IP, HTTP, HTTPS, DNS, SMTP, FTP, SSH), Опыт работы с системами управления рисками, Опыт работы с различными типами баз данных (SQL, NoSQL)
E6	Консультант по безопасности	T1583.002	Знание протоколов сетевой безопасности (TCP/IP, HTTP, HTTPS, DNS, SMTP, FTP, SSH), Опыт работы с технологиями безопасности приложений (Application Security), Опыт работы с системами безопасности мобильных приложений (MAM), Опыт работы с системами безопасности веб-приложений (WAF), Опыт работы с системами защиты от вредоносного ПО, Опыт работы с различными типами приложений (веб, мобильные, десктопные), Разработка планов реагирования на инциденты безопасности (IRP), Умение эффективно общаться с клиентами и предоставлять им консультации, Понимание принципов работы различных систем и технологий, Понимание принципов работы различных систем и технологий
E6	Консультант по безопасности	T1003	Опыт работы с различными инструментами для анализа безопасности, Опыт работы с различными инструментами для анализа рисков, Опыт работы с различными инструментами для анализа безопасности (Nessus, Nmap, Burp Suite), Опыт работы с системами управления доступом (IAM), Разработка политик безопасности информации, Опыт проведения обучения по вопросам информационной безопасности, Опыт проведения аудита информационной безопасности, Опыт разработки и внедрения систем управления доступом (IAM), Опыт работы с системами управления информационной безопасностью (ISMS), Опыт работы с системами мониторинга безопасности (SIEM)

E7	Менеджер по ИБ	T1189	Навыки работы с системами управления безопасностью приложений (Application Security Management), Опыт работы с системами управления доступом (Access Control Systems), Навыки работы с системами управления контентом (Content Management Systems), Опыт работы с системами управления версиями (Version Control Systems), Знание методов и инструментов управления доступом к информационным ресурсам, Умение разрабатывать и внедрять программы защиты от несанкционированного доступа, Опыт работы с системами управления идентификацией и доступом (IAM), Навыки работы с системами управления правами доступа (RBAC), Умение разрабатывать и внедрять программы защиты от внешних атак, Знание методов и инструментов защиты информации в системах управления бизнес-процессами (BPM)
E7	Менеджер по ИБ	T1553	Умение разрабатывать и внедрять программы обучения и повышения квалификации сотрудников в области информационной безопасности, Знание методов и инструментов защиты информации в системах управления производством (Manufacturing Execution System), Умение разрабатывать и внедрять программы защиты от шпионажа, Умение разрабатывать и внедрять программы защиты от мошенничества, Умение разрабатывать и внедрять программы защиты конфиденциальной информации, Умение разрабатывать и внедрять программы защиты от утечек данных, Умение разрабатывать и внедрять программы защиты от кражи данных, Умение разрабатывать и внедрять программы защиты персональных данных, Умение разрабатывать и внедрять программы защиты от несанкционированного доступа, Умение разрабатывать и внедрять программы защиты от кибершпионажа
E7	Менеджер по ИБ	T1021.001	Навыки работы с системами управления качеством обслуживания (Service Quality Management), Опыт работы с системами управления доступом (Access Control Systems), Опыт работы с системами управления идентификацией и доступом (IAM), Знание методов и инструментов управления доступом к информационным ресурсам, Навыки работы с системами управления правами доступа (RBAC), Умение разрабатывать и внедрять программы защиты от несанкционированного доступа, Умение разрабатывать и внедрять программы защиты от вирусов и вредоносного ПО, Опыт работы с системами управления знаниями (Knowledge Management Systems), Навыки работы с системами управления информацией (Information Management Systems), Опыт работы с системами управления рисками (Risk Management)

E7	Менеджер по ИБ	T1566	Умение разрабатывать и внедрять программы защиты от фишинга и спама, Умение разрабатывать и внедрять программы защиты от социального инжиниринга, Знание методов и инструментов защиты информации в социальных сетях и мессенджерах, Опыт работы с системами управления идентификацией и доступом (IAM), Навыки работы с системами управления качеством обслуживания (Service Quality Management), Знание методов и инструментов защиты информации в системах управления персоналом (HRMS), Знание методов и инструментов управления доступом к информационным ресурсам, Опыт работы с системами управления доступом (Access Control Systems), Навыки работы с системами управления безопасностью приложений (Application Security Management), Опыт работы с системами управления знаниями (Knowledge Management Systems)
E7	Менеджер по ИБ	T1584.005	Навыки работы с системами управления качеством обслуживания (Service Quality Management), Умение проводить тесты на проникновение (penetration testing), Знание методов и инструментов защиты информации в сетях передачи данных, Знание методов и инструментов защиты информации в социальных сетях и мессенджерах, Опыт работы с системами управления знаниями (Knowledge Management Systems), Навыки работы с системами управления информацией (Information Management Systems), Опыт работы с системами управления рисками (Risk Management), Опыт работы с системами управления проектированием (Design Management Systems), Опыт работы с системами управления требованиями (Requirements Management), Опыт работы с системами управления активами (Asset Management)
E7	Менеджер по ИБ	T1560	Знание методов и инструментов защиты информации в сетях передачи данных, Умение разрабатывать и внедрять программы защиты персональных данных, Умение разрабатывать и внедрять программы защиты от кражи данных, Умение разрабатывать и внедрять программы защиты от утечек данных, Опыт работы с системами предотвращения утечек данных (DLP), Знание методов и инструментов защиты информации в системах управления производственными процессами (SCADA), Умение анализировать и обрабатывать большие объемы данных в контексте информационной безопасности, Навыки работы с системами обнаружения и предотвращения вторжений (IDS/IPS), Знание методов и инструментов защиты информации в финансовых системах, Знание методов и инструментов защиты информации в системах управления контрактами (Contract Management Systems)

E7	Менеджер по ИБ	T1190	Знание методов и инструментов защиты информации в мобильных устройствах, Опыт работы с системами управления идентификацией и доступом (IAM), Опыт работы с системами управления доступом (Access Control Systems), Знание методов и инструментов защиты информации в сетях передачи данных, Знание методов и инструментов управления доступом к информационным ресурсам, Знание методов и инструментов защиты информации в социальных сетях и мессенджерах, Навыки работы с системами управления безопасностью приложений (Application Security Management), Умение разрабатывать и внедрять программы защиты критической инфраструктуры, Умение разрабатывать и внедрять программы защиты от несанкционированного доступа, Опыт работы с системами управления конфигурациями и изменениями (CMDB)
E7	Менеджер по ИБ	T1583.002	Опыт работы с системами управления доступом (Access Control Systems), Опыт работы с системами управления версиями (Version Control Systems), Навыки работы с системами управления безопасностью приложений (Application Security Management), Навыки работы с системами управления правами доступа (RBAC), Знание методов и инструментов защиты информации в системах управления производственными процессами (SCADA), Умение разрабатывать и внедрять программы защиты от вирусов и вредоносного ПО, Навыки работы с системами управления инцидентами (IRM), Умение разрабатывать и внедрять процедуры реагирования на инциденты информационной безопасности, Опыт работы с системами управления знаниями (Knowledge Management Systems), Навыки работы с системами управления информацией (Information Management Systems)
E7	Менеджер по ИБ	T1003	Знание методов и инструментов управления доступом к информационным ресурсам, Умение разрабатывать и внедрять программы обучения и повышения квалификации сотрудников в области информационной безопасности, Опыт работы с системами управления доступом (Access Control Systems), Знание методов и инструментов защиты информации в финансовых системах, Умение разрабатывать и внедрять программы защиты от несанкционированного доступа, Знание методов и инструментов защиты информации в системах управления логистикой (Logistics Management System), Знание методов и инструментов защиты информации в системах управления контрактами (Contract Management Systems), Знание методов и инструментов защиты информации в системах управления закупками (Procurement Management System), Знание методов и инструментов защиты информации в системах управления складскими запасами (Warehouse Management System), Знание методов и инструментов защиты информации в системах управления техническим обслуживанием (Maintenance Management Systems)

E8	Разработчик ПО	T1189	Умение защищать приложения от уязвимости в обработке пользовательского ввода (User Input Handling Vulnerabilities Prevention), Знание методов защиты от XSS-атак (Cross-Site Scripting Prevention), Умение защищать приложения от использования небезопасных компонентов (Using Components with Known Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке файлов (File Handling Vulnerabilities Prevention), Умение защищать приложения от утечек информации через HTTP-заголовки (HTTP Header Information Leakage Prevention), Умение защищать приложения от SQL-инъекций (SQL Injection Prevention), Умение защищать приложения от уязвимости в обработке HTTP/2 (HTTP/2 Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке потоков (Thread Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке указателей (Pointer Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке BGP (BGP Handling Vulnerabilities Prevention)
E8	Разработчик ПО	T1553	Умение защищать приложения от уязвимости в обработке сертификатов (Certificate Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке пользовательского ввода (User Input Handling Vulnerabilities Prevention), Умение обеспечивать безопасность сессий и куки (Session and Cookie Security), Умение защищать приложения от уязвимости в обработке файлов (File Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке файлового дескриптора (File Descriptor Handling Vulnerabilities Prevention), Умение предотвращать CSRF-атаки (Cross-Site Request Forgery Prevention), Знание методов защиты от уязвимости в обработке запросов (Request Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке времени (Time Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке FTP (FTP Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке RTP (RTP Handling Vulnerabilities Prevention)
E8	Разработчик ПО	T1021.001	Умение защищать приложения от уязвимости в обработке пользовательского ввода (User Input Handling Vulnerabilities Prevention), Умение защищать приложения от использования небезопасных компонентов (Using Components with Known Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке идентификаторов сеансов (Session ID Handling Vulnerabilities Prevention), Знание методов защиты от недостаточной аутентификации и авторизации (Broken Authentication and Session Management Prevention), Умение обеспечивать безопасность сессий и куки (Session and Cookie Security), Знание стандартов и лучших практик OWASP (Open Web Application Security Project), Знание методов защиты от уязвимости в управлении секретами (Secrets Management Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке временных меток (Timestamp Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке метаданных (Metadata Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке данных (Data Processing Vulnerabilities Prevention)

E8	Разработчик ПО	T1566	Умение защищать приложения от уязвимости в обработке потоков (Thread Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в управлении ключами (Key Management Vulnerabilities Prevention), Знание методов защиты от уязвимости в управлении секретами (Secrets Management Vulnerabilities Prevention), Знание методов защиты от недостаточной аутентификации и авторизации (Broken Authentication and Session Management Prevention), Умение защищать приложения от уязвимости в обработке файлов (File Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке пользовательского ввода (User Input Handling Vulnerabilities Prevention), Умение защищать приложения от использования небезопасных компонентов (Using Components with Known Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке файлового дескриптора (File Descriptor Handling Vulnerabilities Prevention), Умение обеспечивать безопасность сессий и куки (Session and Cookie Security), Умение защищать приложения от уязвимости в обработке метаданных (Metadata Handling Vulnerabilities Prevention)
E8	Разработчик ПО	T1584.005	Знание методов защиты от уязвимости в обработке сетевых соединений (Network Connection Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке HTTP/2 (HTTP/2 Handling Vulnerabilities Prevention), Знание методов защиты от недостаточной аутентификации и авторизации (Broken Authentication and Session Management Prevention), Умение защищать приложения от уязвимости в обработке метаданных (Metadata Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке данных (Data Processing Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке ответов (Response Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке запросов (Request Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке файлов (File Handling Vulnerabilities Prevention), Знание методов защиты от неправильной обработки исключений (Improper Error Handling Prevention), Умение защищать приложения от уязвимости в обработке пользовательского ввода (User Input Handling Vulnerabilities Prevention)
E8	Разработчик ПО	T1560	Знание методов защиты от уязвимости в обработке данных (Data Processing Vulnerabilities Prevention), Умение защищать приложения от использования небезопасных компонентов (Using Components with Known Vulnerabilities Prevention), Умение защищать приложения от утечек информации через HTTP-заголовки (HTTP Header Information Leakage Prevention), Знание методов защиты от уязвимости в обработке запросов (Request Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке времени (Time Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке DHT (DHT Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке OSPF (OSPF Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке временных меток (Timestamp Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке ARP (ARP Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке RTP (RTP Handling Vulnerabilities Prevention)

E8	Разработчик ПО	T1190	Знание методов защиты от уязвимости в обработке сетевых соединений (Network Connection Handling Vulnerabilities Prevention), Знание стандартов и лучших практик OWASP (Open Web Application Security Project), Умение защищать приложения от уязвимости в управлении ключами (Key Management Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке SSH (SSH Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке метаданных (Metadata Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в управлении секретами (Secrets Management Vulnerabilities Prevention), Умение защищать приложения от SQL-инъекций (SQL Injection Prevention), Умение защищать приложения от логических уязвимостей (Business Logic Flaws Prevention), Знание методов защиты от недостаточной аутентификации и авторизации (Broken Authentication and Session Management Prevention), Умение защищать приложения от уязвимости в обработке HTTP/2 (HTTP/2 Handling Vulnerabilities Prevention)
E8	Разработчик ПО	T1583.002	Знание методов защиты от уязвимости в обработке DNS-запросов (DNS Query Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке ответов (Response Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке HTTP/2 (HTTP/2 Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке файлов (File Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке ICMPv6 (ICMPv6 Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке сокетов (Socket Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке SIP (SIP Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке метаданных (Metadata Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке сертификатов (Certificate Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке контекста (Context Handling Vulnerabilities Prevention)
E8	Разработчик ПО	T1003	Умение обеспечивать безопасность сессий и куки (Session and Cookie Security), Умение защищать приложения от утечек информации через HTTP-заголовки (HTTP Header Information Leakage Prevention), Умение защищать приложения от уязвимости в обработке HTTP/2 (HTTP/2 Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в управлении ключами (Key Management Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке временных меток (Timestamp Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке метаданных (Metadata Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке данных (Data Processing Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке ответов (Response Handling Vulnerabilities Prevention), Знание методов защиты от уязвимости в обработке запросов (Request Handling Vulnerabilities Prevention), Умение защищать приложения от уязвимости в обработке файлов (File Handling Vulnerabilities Prevention)

Таблица 8 – Описание функций выбранных СЗИ

id Техники	Требования к сотрудникам	Название СЗИ	Функции СЗИ
T1189	Знание политики безопасности компании, соблюдение правил работы с конфиденциальными данными.	Система веб-фильтрации	Блокировка доступа к нежелательным веб-сайтам.
T1553	Понимание угроз информационной безопасности, умение распознавать социальную инженерию.	Security Awareness Training Program	Программа обучения сотрудников информационной безопасности.
T1021.001	Знание политик безопасности компании, умение использовать средства защиты информации.	Secure Remote Access Solution	Безопасный удаленный доступ к корпоративным ресурсам.
T1566	Осторожное обращение с электронными письмами, проверка вложений.	Email Security System	Защита электронной почты от спама, вирусов и фишинга.
T1584.005	Знание внутренних регламентов компании, умение работать с системой отчетности.	Система защиты от DDoS-атак	Защита от распределенных атак типа «отказ в обслуживании».
T1560	Знание основ криптографии, умение использовать средства шифрования.	Data Encryption System	Шифрование данных для защиты конфиденциальной информации.
T1190	Знание правил работы с корпоративной сетью, соблюдение политики доступа к данным.	Network Access Control (NAC) System	Контроль доступа к сети.
T1583.002	Знание правил безопасной работы в интернете, умение распознавать фишинг.	DNS Security System	Защита DNS от атак.
T1003	Соблюдение политики паролей, использование сложных и уникальных паролей.	Password Management System	Управление паролями и обеспечение их безопасности.