|  |  |
| --- | --- |
|  | |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ | |
| Федеральное государственное автономное образовательное учреждение высшего образования | |
| **«Дальневосточный федеральный университет» (ДВФУ)** | |
| **Институт математики и компьютерных технологий** | |
| **Департамент информационных и компьютерных систем** | |
| **ОТЧЁТ** | |
| по лабораторной работе №10\_1  на тему  «Солар Дозор» | |
| по дисциплине «Информационная безопасность» | |
| направление «Прикладная информатика в экономике» | |
|  | |
|  | Выполнил студент группы  Б9121–09.03.03пиэ/2  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В. Ю. Туровец |
| Проверил профессор  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С. Г. Фадюшин  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  оценка |
| Г. Владивосток  2024г. | |

# Условие задачи

Цель работы: ознакомиться с программным обеспечением по кибербезопасности на сайте компании Ростелеком-Солар. Основные сведения законспектировать.

1. **Ход работы**

Solar Dozor — это комплексная система предотвращения утечек информации (Data Loss Prevention, DLP), разработанная российской компанией «Ростелеком-Солар». Она предназначена для защиты конфиденциальных данных организаций, обеспечивая мониторинг, контроль и предотвращение их несанкционированного распространения как внутри компании, так и за её пределами. Solar Dozor построен на принципах анализа поведения пользователей, контроля каналов передачи данных и оперативного реагирования на инциденты информационной безопасности.

Основной задачей системы Solar Dozor является выя выявление и предотвращение утечек конфиденциальной информации. Утечками могут является коммерческая тайна, персональные данные клиентов и сотрудников, интеллектуальная собственность и данные, регулируемые законодательством (например, в рамках GDPR, ФЗ-152). Solar Dozor предоставляет возможность перехвата, анализа и блокировки данных на ключевых каналах связи: электронной почте, мессенджерах, социальных сетях, веб-почте, облачных хранилищах, локальных файловых серверах, периферийных устройствах, таких как принтеры и сканеры, а также в буфере обмена.

Solar Dozor включает широкий спектр функциональных модулей, позволяющих повысить эффективность защиты данных.

Модуль перехвата данных осуществляет мониторинг сетевого трафика, анализирует отправляемые файлы и сообщения. Он поддерживает интеграцию с почтовыми серверами, прокси-серверами и системами удалённого доступа.

Модуль анализа поведения пользователей (UBA) использует машинное обучение и запатентованные алгоритмы для изучения действий сотрудников, что позволяет выявлять аномалии, такие как резкое увеличение активности или попытки доступа к запрещённым данным.

Dozor Detective является инструментом для расследования инцидентов, предоставляющим детализированную информацию о действиях сотрудников, включая запись видео с экранов, снимки экрана, запись звука и текстовую расшифровку разговоров.

Модуль интеллектуального анализа документов (IDM) распознаёт содержимое файлов, даже если они зашифрованы или преобразованы в нестандартные форматы, что позволяет выявлять утечки по контенту, а не только по метаданным.

Модуль MultiConnector обеспечивает интеграцию с другими системами безопасности, такими как SIEM, SOAR, XDR и IRP, для расширения возможностей мониторинга и реагирования.

Система поддерживает контроль работы с периферийными устройствами, такими как USB-накопители, мобильные устройства, сканеры и принтеры. Например, она может блокировать копирование файлов на флешки или отправку документов на печать без соответствующего разрешения. Также Solar Dozor предоставляет возможность блокировки отправки файлов через небезопасные Wi-Fi-сети или общественные точки доступа.

Solar Dozor сертифицирован ФСТЭК России по 4-му уровню доверия, что делает её соответствующей требованиям государственных стандартов информационной безопасности. Она включена в Единый реестр отечественного программного обеспечения, что позволяет использовать её в рамках политики импортозамещения. Система совместима с российскими операционными системами (Astra Linux, РЕД ОС) и СУБД, что дополнительно подтверждает её актуальность в условиях санкций.

Solar Dozor предоставляет централизованный веб-интерфейс, который позволяет администраторам управлять всеми функциями системы из одного окна. Это упрощает настройку политик безопасности, отслеживание инцидентов и обновление системы. Благодаря масштабируемости Solar Dozor успешно применяется в крупных компаниях с территориально распределённой структурой, поддерживая мониторинг на десятках тысяч рабочих станций.

Система активно обновляется и развивается. Последние версии включают такие функции, как распознавание QR-кодов, что позволяет предотвратить фишинговые атаки, связанные с использованием мошеннических кодов. Добавлена возможность контроля подключения сотрудников к незащищённым сетям, а также записи видео с экранов рабочих станций, что помогает при расследовании инцидентов.

Solar Dozor также интегрируется с модулями управления инцидентами, предоставляя данные для анализа причин утечек и обучения сотрудников правилам информационной безопасности. Она поддерживает гибкое создание политик безопасности с учётом специфики отрасли, будь то финансы, медицина, промышленность или государственный сектор.