Управление информационной безопасностью бизнеса

Модуль 1. Регламентные документы в сфере информационной безопасности

Лекция 8

Системы мониторинга, анализа и учета компьютерных инцидентов.

проф. Бойченко О.В.

Симферополь, 2023

Вопросы:

1. Мониторинг информационной безопасности;
2. Средства и системы мониторинга информационной безопасности.

Литература:

Бойченко О.В. Информационная безопасность : учебное пособие./ Бойченко О. В., Журавленко Н.И. – Симферополь, 2016. – 248 с.

Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.

Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и Техника, 2004. – 384 с.

Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. – М.: Юниор, 2003. – 504 с.

Галатенко В. А. Основы информационной безопасности**. –** М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2008. – 208 с.

- **Введение**

Одним из наиболее эффективных путей **предупреждения** нарушения устойчивого функционирования информационных/автоматизированных систем и/или нарушения конфиденциальности, целостности и доступности обрабатываемой в них информации **является постоянный контроль (мониторинг)** их состояния и поступающих в систему данных с целью своевременного выявления инцидентов информационной безопасности, связанных в том числе с реализацией компьютерах атак, и оперативного реагирования на них.

Реализацию указанных процессов при обеспечении безопасности объектов критической информационной инфраструктуры (ОКИИ) РФ обеспечивает **государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА).** При этом процессы выявления инцидентов информационной безопасности и реагирования на них, включая состав анализируемых параметров системы и возникающих в ней событий, **разрабатываются участниками ГосСОПКА самостоятельно** с учетом отраслевой специфики, особенностей функционирования конкретных ОКИИ и разработанных **национальным координационным центром**

1. Мониторинг информационной безопасности

Мониторинг - система постоянного наблюдения за явлениями и процессами, проходящими в окружающей среде и обществе, результаты которого служат для обоснования управленческих решений по обеспечению безопасности людей и объектов экономики.

Системы мониторинга контролируют технологии, используемые компанией (оборудование, сети и коммуникации, операционные системы или приложения и т. д.), для анализа их работы и производительности, а также для обнаружения и предупреждения о возможных ошибках.

Собственно производится **мониторинг** производительности сетевых интерфейсов и устройств:

1. сбор статистических данных по загрузке и числу ошибок;
2. формирование отчетности и прогнозов;
3. управление конфигурациями сетевого оборудования - автоматизация управления ими.

Основная задача систем мониторинга – отслеживание компьютерных инцидентов. **Компьютерный инцидент** - факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации.

Инциденты могут быть как **умышленными, так и непреднамеренными**. Если обратить внимание на первый вид инцидента, то он может быть спровоцирован разными средствами, техническим взломом или намеренным инсайдом. Оценить масштабы влияния на безопасность и последствия атаки крайне сложно. Это может быть: раскрытие или изменение украденной информации, нанесение ущерба активам компании или их полное хищение и т. д. Основные примеры: **Отказ в обслуживании**.

Уровни опасности измеряют влияние инцидента на компанию.

Опасность	Описание
1	Критически опасный инцидент с очень большими последствиями
2	Серьезный инцидент со значительными последствиями
3	Несерьезный инцидент с незначительными последствиями

Таким образом, основными функциями мониторинга являются: - наблюдения; - оценка; - прогноз; - разработка рекомендаций.

Методы мониторинга

Метод	Применение
Наблюдение и личное участие	Определение необходимых и имеющихся знаний и навыков
Опросы, обсуждения	При неожиданном возникновении сложных проблем в текущих вопросах
Анкетирование	Определение необходимых и имеющихся знаний и навыков.
Изучение документов	Оценка понимания задач

Для чего необходим мониторинг информационной безопасности?

Во время своей работы практически все компании регулярно подвергаются угрозам, связанным с несанкционированным доступом к корпоративным информационным ресурсам.

Среди таких угроз наиболее часто встречающиеся – это атаки хакеров и распространение вредоносного ПО, однако риски информационной безопасности могут появляться и со стороны самих сотрудников.

Низкий уровень компьютерной грамотности, устаревшее или уязвимое программное обеспечение, даже использование облачных сервисов или услуг сторонних IT-провайдеров могут нести угрозы, из которых самой серьезной является утечка или подмена коммерчески значимых данных.

Так как подобные риски являются сегодня широко распространенными, и полностью исключить их нельзя, большое значение приобретает оперативное выявление подобных угроз и быстрое реагирование на них. Реализовать это возможно, используя средства мониторинга информационной безопасности. Работая в непрерывном автоматическом режиме, данные средства значительно снижают шанс несанкционированных действий остаться незамеченными.

Таким образом, **мониторинг информационной безопасности** представляет собой сбор, систематизирование и анализ сведений о состоянии корпоративной сети и поведении ее пользователей.

Основная цель такого анализа заключается **в выявлении** несанкционированных действий самих сотрудников или посторонних лиц, проникших в сеть. Современные системы мониторинга информационной безопасности позволяют **обнаруживать такие действия и выдавать соответствующие уведомления**, помогая тем самым своевременно пресекать риски.

Что такое мониторинг событий информационной безопасности (ИБ)?

С технической точки зрения это процесс автоматизированной проверки всех событий безопасности, которые система получает из ряда источников.

Такими источниками являются:

Журналы ОС	**Антивирусные приложения**	**ПО, анализирующее защищенность инфраструктуры**	**Сетевое оборудование**

На сегодняшний день существует ряд решений для обеспечения постоянного отслеживания угроз. Любая система мониторинга событий информационной безопасности может быть отнесена к одной из следующих категорий:

SIEM (Security Information and Event Management) – системы, которые отслеживают и анализируют события в режиме реального времени.

UBA (User Behavioral Analytics) – системы, которые собирают данные о действиях сетевых пользователей с целью последующего анализа и выявления возможных угроз.

UEBA (User and Entity Behavioral Analytics) – системы, позволяющие обнаруживать аномалии в действиях пользователей и работе самих корпоративных сетей.

- **Решения, контролирующие эффективность сотрудников и отслеживающие внутри сети все их действия**, которые касаются работы с корпоративными конфиденциальными данными.
- **Системы поиска и выявления различного рода атак**, ориентированные на улучшение общей защищенности корпоративной сети.

основные компоненты систем мониторинга информационной безопасности

Системы данного класса, как правило, включают в себя следующие основные компоненты:

Программные агенты	**Сервер**	**Хранилища информации**
Консоль	**Персонал, работающий с системой**	**Регламенты работы по мониторингу**

- программные агенты – их задача заключается в сборе данных, поступающих из различных источников,

- сервер – выполняет централизованный анализ поступившей информации, основываясь на тех правилах и политиках, которые были заданы ИБ-специалистом,

- хранилища информации – консолидируют данные обо всех событиях безопасности, поступающих из источников. Информация в хранилище может содержаться от нескольких дней до нескольких месяцев, в зависимости от размера самого хранилища и объемов поступающих данных,

- консоль – служит для управления параметрами обработки, просмотра журналов событий и обращения к хранилищу,

- персонал, работающий с системой,

- регламенты работы по мониторингу.

2. Средства и системы мониторинга информационной безопасности.

Для того, чтобы настроить мониторинг информационной безопасности средств и систем информатизации, необходимо определить ряд параметров:

что должно рассматриваться в качестве инцидента ИБ,

какие виды инцидентов присущи или могут быть присущи данной компании,

какие события могут предварять каждый тип инцидента,

какие источники могут производить инциденты,

к каким рискам ведет каждый вид инцидента, и каков взаимный приоритет данных рисков.

В каждой компании определение этих параметров и настройка систем мониторинга индивидуальны. Выбор самой системы предполагает учет таких нюансов, как планируемое количество источников событий для обработки, возможности системы по анализу поступающих событий, функционал визуализации и детализации отчетов. Сегодня на рынке существует широкий выбор решений для мониторинга ИБ, как отечественных, так и зарубежных, среди которых – системы от Cisco, McAfee, Fortinet и др.

Для целей предотвращения угроз, выявляемых в ходе мониторинга, создается SOC (Security Operations Center – Центр по обеспечению безопасности) SOC представляет собой команду специалистов по инфобезопасности, основная задача которых – выявлять и предотвращать угрозы корпоративным данным.

Мониторинг состояния информационной безопасности дает возможность в автоматическом режиме анализировать работу IT-ресурсов компании, сетевых приложений, оборудования и веб-сервисов. Применение специализированных решений для мониторинга позволяет эффективно управлять рисками и обеспечивать соответствие всех систем корпоративным политикам информационной безопасности.

В тоже время некорректно настроенная, пусть и дорогая, система мониторинга ИБ не позволит снизить потери от негативных инцидентов ИБ. Поэтому рекомендуется проводить ее аудит не реже одного раза в год.

Анализ требований к составу передаваемой в ГосСОПКА информации о выявленных в ОКИИ инцидентах информационной безопасности и полей разработанного НКЦКИ формата представления информации об инциденте позволяет сделать вывод о том, что в качестве инцидентов рассматриваются последствия:

преднамеренных атак, проводимых с использованием каналов связи;

внедрения вредоносного программного обеспечения;

неосторожных или неквалифицированных действий персонала, ограниченных случаем непреднамеренного отключения ОКИИ.

Исходя из описания перечисленных инцидентов для их выявления необходимо проводить постоянный автоматизированный сбор и анализ событий (на основе правил корреляции), поступающих из средств анализа сетевого трафика, обнаружения (предотвращения) атак, антивирусной защиты и поведенческого анализа программного обеспечения, использующих сигнатурные методы анализа и методы машинного обучения.

Недостаток описанного подхода состоит в том, что в качестве инцидентов не рассматриваются последствия сбоев в программных и/или аппаратных компонентах системы, вызванные в том числе воздействием внешних факторов (отказами систем кондиционирования, электропитания и др.).

Такие сбои в сочетании с недостатками в архитектуре или настройках системы в целом или отдельных ее компонентов часто приводят к нарушению или существенному снижению эффективности их функционирования. В этом случае события, связанные с развитием инцидента, принципиально не могут быть зарегистрированы по результатам анализа сетевого трафика или анализа поведения программных компонентов антивирусными средствами.

В результате инцидент может быть обнаружен не сразу и только по косвенным признакам (например, жалобам пользователей на снижение быстродействия), а его локализация и устранение последствий при отсутствии априорной информации об отказах в некоторых случаях может занять значительное время, что особенно критично для ОКИИ.

С целью **устранения** указанного недостатка предлагается дополнить категорию событий «Нарушение или замедление работы контролируемого информационного ресурса (availability)» типом события «Отказ аппаратных/программных компонентов ОКИИ (software/hardware fault)», которое по своей сути является инцидентом типа «отказ в обслуживании», не связанным с проведением атак [4]. Для обеспечения возможности выявления данного типа инцидентов информационной безопасности в качестве источников событий для их последующего анализа следует применять автоматизированные системы мониторинга (сбора и анализа событий) инфраструктуры ОКИИ, позволяющие контролировать:

текущие и усредненные значения параметров производительности (загрузку CPU, RAM, накопителей, операции чтения/записи, скорость передачи данных и др.);

статус аппаратных компонентов (состояние сетевых интерфейсов, блоков питания, вентиляторов и др.);

изменения конфигурационных файлов;

изменения версий программного обеспечения.

Контроль указанных параметров может осуществляться путем взаимодействия с агентами системы мониторинга, устанавливаемыми в совместимых операционных системах, или с использованием протокола SNMP: активного опроса устройств (серверов, телекоммуникационного оборудования,

Состав конкретных контролируемых параметров и событий должен формироваться на этапе инвентаризации ОКИИ с учетом как технических возможностей применяемых в них программных и аппаратных средств (версий системного и прикладного программного обеспечения, поддерживаемых протоколов и пр.), так и возможностей используемых систем мониторинга.

В качестве примера можно привести особенности использования протокола SNMP для мониторинга телекоммуникационного оборудования:

- состав и коды (OID) передаваемых в сообщениях SNMP событий определяются базами MIB и отличаются на устройствах разных производителей. В этом случае по результатам инвентаризации должны быть подготовлены совместимые с применяемой системой мониторинга описания параметров и событий и их сопоставление с кодами событий (OID), передаваемых в сообщениях SNMP.

Стоит отметить, что при выборе системы мониторинга (сбора событий) должны быть учтены ее возможности по автоматизированной нормализации всех регистрируемых событий: они должны передаваться для дальнейшей регистрации и анализа (например, в SIEM-систему) в заранее определенном формате.

Предложенная модификация известного подхода к разработке процессов выявления инцидентов информационной безопасности и реагирования на них позволит:

1. своевременно выявлять сбои в программных и/или аппаратных компонентах системы, приводящие к возникновению инцидентов типа «отказ в обслуживании», не связанных с реализацией атак;

2. разрабатывать более точные и надежные правила корреляции за счет увеличения общего числа анализируемых параметров систем и возникающих событий (учета дополнительных признаков атак, таких как аномальное изменение параметров производительности устройств, изменения их конфигурации и др.) и тем самым снизить количество ложных срабатываний;

3. увеличить объем данных о состоянии ОКИИ в момент выявления инцидента для их всестороннего анализа и установления причин инцидента на этапе реагирования, в том числе с привлечением экспертов НКЦКИ;

4. по результатам проведенной инвентаризации ОКИИ осуществить обоснованный подбор технических решений (систем сбора событий, SIEM-систем и др.), соответствующих всем требованиям, предъявляемым к выявлению инцидентов, и учитывающих специфику функционирования конкретных ОКИИ.

Однако стоит учесть, что в случае привлечения экспертов НКЦКИ или иных организаций к анализу инцидента передаваемая в ГосСОПКА дополнительная информация, которая может включать конфиденциальные сведения об ОКИИ, должна в обязательном порядке иметь ограничительный маркер TLP.

Для этого указанный маркер, который по умолчанию имеет значение «TLP:WHITE» («Распространение сведений не ограничено»), в случае необходимости может быть заранее присвоен определенным параметрам или событиям, регистрируемым системой мониторинга.

Его наличие или отсутствие должно учитываться автоматизированной системой регистрации инцидентов при формировании карточки инцидента и ее отправке в ГосСОПКА:

- если карточка содержит дополнительные данные с маркером TLP, то значение маркера карточки должно соответствовать максимальному значению маркера приложенных данных.

Таким образом, **для своевременного выявления инцидентов информационной безопасности в ОКИИ и оперативного реагирования на них** в состав контролируемых параметров и событий должны входить:

содержание передаваемых по каналам связи сообщений (входящего и исходящего сетевого трафика);

содержание журналов регистрации событий применяемых средств защиты информации: средств защиты от несанкционированного доступа, антивирусной защиты, защиты среды виртуализации, обнаружения (предотвращения) атак, межсетевых экранов и т.п.;

текущие и усредненные значения параметров производительности (загрузку CPU, RAM, накопителей, операции чтения/записи, скорость передачи данных и др.) серверов, телекоммуникационного оборудования, межсетевых экранов и др.;

статус аппаратных компонентов (состояние сетевых интерфейсов, блоков питания, вентиляторов и др.) серверов, телекоммуникационного оборудования, межсетевых экранов и др.;

изменения конфигурационных файлов и версий программного обеспечения серверов, телекоммуникационного оборудования, межсетевых экранов и др.

Для их сбора, предварительного анализа и нормализации в состав системы мониторинга помимо автоматизированных средств анализа информации (средств обнаружения атак, SIEM-систем и др.) и регистрации инцидентов должны входить автоматизированные средства контроля параметров программных и аппаратных компонентов инфраструктуры ОКИИ и связанных с их функционированием

Makves IRP предоставляет сотрудникам службы безопасности удобный инструмент для регистрации инцидентов, управления их жизненным циклом и создания типовых сценариев реагирования на события.

Инциденты могут быть получены из внешних систем (SIEM, IDM, DLP и другие продукты), а также открыты вручную. Такой подход позволяет создать единую базу данных для всех значимых событий безопасности, быстро распределять их среди ответственных сотрудников, контролировать и анализировать процесс обработки инцидентов.

Задача - автоматизировать процесс менеджмента событий в сфере информационной и экономической безопасности

Карточка инцидента в Makves IRP содержит:

Категорию события

Возможность анализировать происшествия в разрезе их типов

Сценарий

Описание действий, которые необходимо выполнить в случае возникновения инцидента

Приоритет

Позволяет настраивать и устанавливать важность события

Статус

Описывает текущий этап обработки инцидента — анализ, устранение, восстановление и т. д.

Исполнителя

Отображает исполнителя, назначенного для обработки события

Тему и описание инцидента

Описывают детальную информацию о происшествии

Каждому инциденту можно назначить срок расследования и добавить пользователей, которые будут контролировать процесс работы с ним.

Вместе с событием можно хранить связанные объекты, полученные из Makves DCAP, а также необходимые файлы.

Для каждого инцидента Makves IRP ведет журнал событий, в который попадают все действия с карточкой.

Информация обо всех инцидентах собирается в удобной и настраиваемой панели управления.

При помощи графических информеров администратор системы может получать информацию о количестве событий, находящихся в работе, детализировать ее по типам нарушений, их статусам и ответственным сотрудникам.

Исполнители также могут работать с панелью управления, чтобы отслеживать состояние назначенных им инцидентов.

Ключевые преимущества Makves IRP

- **Регистрация нарушений**

- **фиксирует все виды нарушений в единой базе данных — информационные, инфраструктурные, режимные и другие.**

- **Удобная система отчетности**

- **с возможностью вывода статистики в разрезе типов происшествий, их состояния или ответственных сотрудников**

- **Быстрый поиск инцидентов**

- **поиск по сложным запросам дает возможность выявить составные, многоэтапные атаки**

- **Удобный интерфейс**

- **оптимизированный для десктопных и мобильных устройств**

Платформа **AVSOFT LOKI** представляет собой систему сенсоров, которые располагаются в подсетях организации и определяют типы активных устройств в сети путём сканирования.

Далее система в автоматическом режиме подбирает ловушки, которые располагаются рядом с реальными сервисами организации, ожидая подключения злоумышленника.

Кроме ловушек LOKI имеет ещё приманки на рабочих местах пользователей; они представляют собой значимые для атакующего артефакты, такие как учётные данные, сессии посещения.

Также система даёт клиентам возможность создавать собственные ловушки и приманки. Каталог ловушек включает в себя не только серверы и рабочие станции, но и IoT, IIoT, станки, IP-видеокамеры, медицинское оборудование, телефоны и SCADA-системы.

Процесс внедрения платформы состоит из трёх этапов. Сначала производится сканирование существующей инфраструктуры, затем следует развёртывание ловушек, а на последнем этапе выполняется установка приманок.

При наличии признаков атаки AVSOFT LOKI оповещает службу безопасности и начинает собирать данные об атакующем: IP-адрес, команды, артефакты, загруженные файлы и прочее. Включен в реестр отечественного ПО (№11743 от 15.10.2021).

ИКС — надежное российское решение для защиты корпоративной сети, где реализованы разные инструменты, обеспечивающие безопасность данных: межсетевой экран, Web Application Firewall, IPS/IDS -Suricata, встроенные антивирусы и защита от подбора паролей Fail2ban.

Быстрый и мощный межсетевой экран — главный инструмент, обеспечивающий безопасность корпоративной сети. Web Application Firewall используется для безопасности веб-приложений.

Система обнаружения и предотвращения вторжений — детектор атак Suricata позволяет фиксировать, хранить информацию о подозрительной активности, блокировать ботнеты, DoS и DDoS-атаки, TOR, анонимайзеры, P2P и торрент-клиенты.

Встроенные антивирусы обеспечивают общую защиту сети от входящих угроз и вирусов в потоке трафика и в почтовых сообщениях. А встроенный в ИКС Fail2ban защищает сервисы от попыток подбора паролей.

Кроме того, межсетевой экран ИКС — это более 90 функций и сервисов в едином удобном интерфейсе, разработка позволяет оптимизировать работу корпоративной сети, настроить удаленный доступ, контролировать доступ пользователей, настроить фильтрацию контента, развернуть сетевые сервисы.

ИКС включен в реестр отечественного ПО для ЭВМ и БД (№ 322).

Сервис Dr.Web FixIt! предназначен для удаленной диагностики инцидентов информационной безопасности на ОС Windows и устранения их последствий. В отличие от продуктов, предназначенных для обнаружения уже известных (или похожих на известные) вредоносных программ с помощью вирусных баз, Dr.Web FixIt! позволяет выявлять новейшие вредоносные программы, а также программы, используемые для целевых атак и не определяемые никакими иными инструментами.

Работает Dr.Web FixIt! следующим образом: сначала оператор создает задачу в веб-сервисе и отправляет анализирующую утилиту FixIt! владельцу проверяемого компьютера. Тот запускает утилиту, она проверяет компьютер и формирует отчет. Затем оператор анализирует отчет в веб-сервисе, создает лечащую утилиту FixIt! и отправляет ее владельцу проверяемого компьютера. Последний запускает утилиту FixIt!, которая выполняет заданный скрипт и формирует новый отчет.

Dr.Web FixIt! пригодится в целом ряде случаев, в том числе когда необходимо найти вредоносные и подозрительные объекты, которые не обнаруживает обычное сканирование антивирусом; требуется выявить ошибки в настройках антивируса или заражение MBR/VBR; в компании нет собственной SOC-команды; нужно произвести ретроспективный анализ состояния защиты системы, проследить во времени ситуацию и поведение критических сервисов и программ.

Включен в реестр отечественного ПО (№15257 от 25.10.2022).

InfoWatch ARMA — отечественная система промышленной кибербезопасности. Является лучшим в своем классе российским решением по защите ИТ-систем в промышленности (по мнению экспертов национальной премии TAdviser IT Prize в 2022 году).

Помогает объектам КИИ справиться с ключевыми вызовами: защитой от кибератак и ускоренным импортозамещением.

Единая система защищает информацию в промышленных сетях, рабочие станции и сервера, в также обеспечивает централизованное управление средствами защиты и инцидентами ИБ

Решение имеет сертификат ФСТЭК и включено в единый реестр российского ПО Минцифры России

В систему входят 3 продукта:

- InfoWatch ARMA Industrial Firewall. Регистрация № 5937 от 19.11.2019 г.
- InfoWatch ARMA Management Console. Регистрация № 11445 от 20.09.2021 г.
- InfoWatch ARMA Industrial Endpoint. Регистрация № 11521 от 20.09.2021 г.

Межсетевой экран InfoWatch ARMA Industrial Firewall работает с сетевым трафиком и осуществляет глубокий разбор специализированных промышленных протоколов.

Защита рабочих станций и серверов в АСУ ТП обеспечивается благодаря InfoWatch ARMA Industrial Endpoint.

Единый центр управления InfoWatch ARMA Management Console осуществляет сбор событий со средств защиты, формирование инцидентов по преднастроенным правилам корреляции и настройку автоматического реагирования на них. Внедрение системы InfoWatch ARMA позволяет выполнить до 90% технических мер Приказа №239 ФСТЭК России.

InfoWatch Traffic Monitor — российская DLP-система нового поколения, которая с помощью технологий искусственного интеллекта предотвращает утечки конфиденциальной информации, прогнозирует риски и повышает уровень автоматизации работы службы ИБ в условиях быстрых изменений.

В зависимости от задач заказчиков система поставляется вместе со следующими модулями:

- InfoWatch Activity Monitor позволяет увидеть детальную картину рабочего дня сотрудников, собрать доказательную базу по инцидентам информационной безопасности и сформировать отчеты.
- InfoWatch Vision — BI- система для ежедневного мониторинга оперативной обстановки и ускорения расследования.
- InfoWatch Prediction — UBA система на основе технологий искусственного интеллекта помогает автоматически сформировать группы риска на основе динамических моделей поведения каждого сотрудника и увидеть нарушения, которые только готовятся.
- InfoWatch Data Discovery осуществляет аудит хранения данных на файловых ресурсах организации.

DLP-система Traffic Monitor полностью отвечает требованиям импортозамещения. Внесена в реестр отечественного ПО, сертифицирована ФСБ, Министерством обороны, ЦБ РФ, ФСТЭК России. Поддерживает российские операционные системы РЕД ОС, Astra Linux и ALT Linux, базы данных PostgreSQL, PostgreSQL Pro и Postgres Pro Enterprise. InfoWatch Traffic Monitor. Реестровая запись №10340 от 21.04.2021. InfoWatch Activity Monitor. Реестровая запись №10341 от 21.04.2021. InfoWatch Vision. Реестровая запись №10342 от 21.04.2021

- InfoWatch Prediction. Реестровая запись №19043 от 18.09.2023.