



Для оперативной связи с нами вы можете
использовать любой удобный для вас способ:

www.recfaces.ru

+7 495 268 08 93

sales@recfaces.ru

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ ID-LOGON

Id-Logon — программный продукт для биометрической аутентификации пользователей в информационных системах по изображению лица

Id-Logon позволяет выполнить безопасную и удобную беспарольную биометрическую аутентификацию пользователя по изображению лица при организации доступа в различные корпоративные информационные системы. Также решение обеспечивает периодическую проверку статуса пользователя, находящегося перед экраном клиентского устройства в данный момент, с целью определения возможных сценариев ограничения доступа и информирования профильных подразделений информационной безопасности о допущенных нарушениях.

ЧТО ПОЛУЧАЕТ ПОЛЬЗОВАТЕЛЬ РЕШЕНИЯ?

- Безопасную биометрическую аутентификацию пользователей в различных корпоративных информационных системах
- Удобную беспарольную аутентификацию с использованием биометрических данных пользователей
- Дополнительный режим двухфакторной аутентификации: биометрические данные и пин-код/пароль
- Периодическую проверку статуса пользователя, находящегося перед экраном клиентского устройства
- Выполнение различных сценариев ограничения доступа и информирование службы информационной безопасности при несоответствии статуса пользователя
- Оперативное уведомление служб информационной безопасности при работе более чем одного пользователя с клиентским устройством
- Своевременную обработку вызовов от информационных корпоративных и DLP-систем на биометрическую верификацию пользователя, при совершении значимых операций или подозрении на возможную утечку информации
- Наличие готовой интеграции с Microsoft Active Directory, а также возможность интеграции с другими LDAP-каталогами, такими как: Oracle Internet Directory, IBM Tivoli DirectoryServer



УСТАНОВКА РЕШЕНИЯ = 20 МИНУТ

**ЗА 20 МИНУТ ВЫ ПОЛУЧАЕТЕ ГОТОВЫЙ К ИСПОЛЬЗОВАНИЮ ПРОДУКТ
СО ВСЕМИ НЕОБХОДИМЫМИ ФУНКЦИОНАЛЬНЫМИ ВОЗМОЖНОСТЯМИ**

Решение Id-Logon устанавливается на вычислительной инфраструктуре Заказчика, приложения для аутентификации устанавливаются на корпоративных клиентских устройствах. Корпоративные клиентские устройства пользователей оснащаются биометрическими датчиками: стандартными web-камерами или специализированными web-камерами для повышенной устойчивости к контролю компрометации системы и работе в условиях низкой освещенности. Решение имеет отдельный современный графический интерфейс.

Простые пароли и беспарольная аутентификация

Одной из главных проблем, с которой сталкивается специалист по информационной безопасности в организации, является использование слабых или стандартных паролей, которые в подавляющем большинстве случаев уже скомпрометированы. Выполнение тестов на проникновение и компрометацию учетной записи методом перебора паролей является наиболее простым и быстрым вектором атаки, позволяющим «пробить периметр» или получить административные привилегии. Статистика таких атак заставляет задуматься — успешность реализации составляет до 85% случаев, в том числе в крупных корпоративных структурах. Использование беспарольной биометрической аутентификации Id-Logon позволяет выполнить процедуру безопасным для организации и удобным для пользователя и способом.

Беспарольная аутентификация и удобство пользователя

Обратной стороной строгих парольных политик для корпоративных учетных записей, требований по длине создаваемых паролей и наличию в них спецсимволов (строчных и прописных букв, цифр, знаков) является сложность для значительной доли сотрудников систематически запоминать сложные обновленные пароли. В результате сотрудники не находят ничего лучше, как записать новый пароль и оставить эту запись рядом с рабочим местом. В итоге самая строгая корпоративная парольная политика становится жертвой простой человеческой невнимательности и халатности. Id-Logon выполняет беспарольную аутентификацию пользователя с использованием индивидуальных биометрических данных, а встроенные эффективные методы контроля компрометации системы с использованием фото- или видео-материалов позволяют противостоять попыткам взлома и своевременно проинформировать о них специалистов службы информационной безопасности. Таким образом, Id-Logon обеспечивает высокий уровень достоверности результатов аутентификации, при этом процедура проста и удобна для пользователя.

Двухфакторная аутентификация

Дополнительный уровень безопасности — Id-Logon, который гарантирует, что доступ к вашей учетной записи сможете получить только вы, даже если ваш пароль стал известен кому-то еще. В дополнение к вводу пароля или пин-кода система обеспечивает биометрическую верификацию пользователя, которая исключает возможность использования корпоративных информационных ресурсов посторонними.

Проверка наличия пользователя

После авторизации пользователь может на время покинуть рабочее место. Id-Logon выполняет периодическую проверку (в фоновом режиме) статуса пользователя, находящегося перед экраном клиентского устройства после успешной авторизации. Если Id-Logon «не видит» пользователя за клиентским устройством, то увеличивает частоту опроса для биометрической верификации, а через заданный в системе период времени, при отсутствии пользователя, автоматически блокирует доступ.

В случае, если после успешной авторизации пользователя к работе с клиентским устройством приступит другой сотрудник или посторонний человек, система проинформирует сотрудников информационной безопасности об инциденте и может автоматически заблокировать доступ к корпоративным информационным ресурсам.

Одно рабочее место — один сотрудник

Id-Logon позволяет ограничивать права доступа к клиентским устройствам третьим лицам, в частности, за одним клиентским устройством не смогут находиться несколько сотрудников одновременно. Решение автоматически, в фоновом режиме, определит это как нарушение и заблокирует доступ к корпоративным информационным ресурсам. Права доступа определяет администратор системы, для этого в Id-Logon предусмотрены гибкие настройки, позволяющие использовать ролевую модель. В базе биометрических профилей выполняется регистрация сотрудников с последующей привязкой к конкретным клиентским устройствам.

Мобильность

Id-Logon позволяет идентифицировать и верифицировать пользователей при использовании мобильных устройств, таких как смартфоны или планшетные компьютеры. Особенно это важно для компаний, чья деятельность сопряжена с удаленной работой сотрудников без стационарных рабочих мест. Id-Logon позволяет аутентифицировать пользователя мобильного устройства, предоставить или отказать ему в доступе как к самому устройству, так и к конкретному корпоративному приложению. При этом служба информационной безопасности получает информацию об аутентифицированном пользователе мобильного устройства, обеспечив тем самым повышенный уровень защищенности корпоративных данных.

Аналитика и отчетность

В Id-Logon предусмотрена возможность создания отчетов о результатах аутентификации пользователей корпоративных информационных ресурсов и допущенных нарушениях при работе с ними. Например, можно посмотреть количество и статистику нарушений по набору интересующих клиентских устройств, а также получить детальную информацию с указанием параметров нарушения аутентификации или использования корпоративных ресурсов по конкретному нарушению. Предусмотренные в системе фильтры позволяют быстро и удобно сформировать отчет по набору интересующих параметров.

Проверка пользователя по запросу DLP

Совместная работа DLP-систем и Id-Logon позволяет выполнить в фоновом режиме верификацию пользователя по запросу DLP-системы при наличии подозрительных действий, а также при выполнении заданного перечня операций в корпоративных информационных системах. В случае запроса от КИС или DLP-систем Id-Logon выполняет верификацию авторизованного пользователя, а также информирует о нахождении иных сотрудников организации или посторонних лиц.

Подтверждение личности перед совершением значимых операций

По заданному набору значимых операций в корпоративных информационных системах Id-Logon инициирует запуск активной верификации (окно верификации) пользователя для подтверждения личности до совершения операции. Данный режим позволяет удостовериться, что операция совершена уполномоченным сотрудником компании, а также сохранить журнал подтверждения для таких операций.

Открытый API

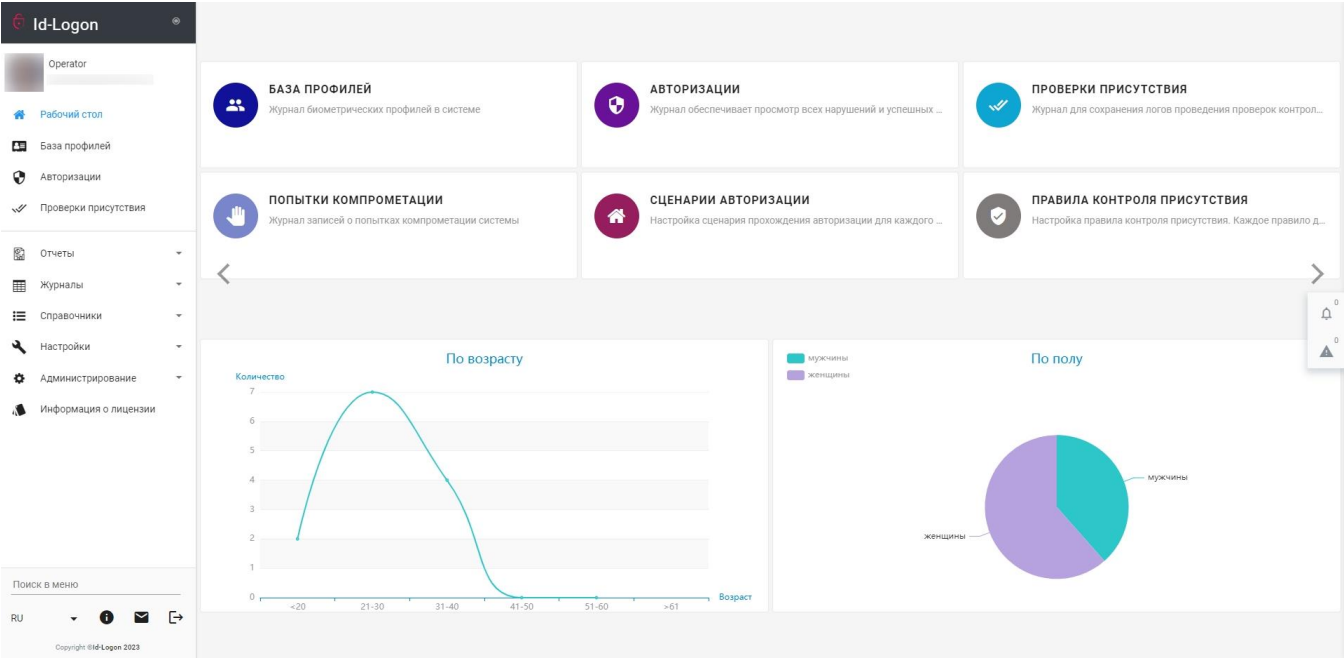
Id-Logon легко интегрируется с различными внешними информационными системами с помощью открытого API.

Союз биометрических решений для повышения безопасности

В портфеле компании РекФэйсис есть специализированное решение для систем контроля и управления доступом — Id-Gate, которое получает и хранит персонифицированную информацию о приходе или уходе сотрудника в организацию. Совместное использование решений Id-Logon и Id-Gate позволяет контролировать выполнение аутентификации сотрудников в информационных системах, а также уведомлять о попытке аутентификации пользователя, информация о приходе которого в организацию отсутствует в системе контроля и управления доступом.

ПРИМЕР ИНТЕРФЕЙСА ID-LOGON

Рабочий стол Id-Logon



База профилей Id-Logon

The screenshot shows the 'База профилей' (Profiles Database) interface. It includes a search bar, filters, and a table of profiles. The table has columns for фото (photo), Пол (gender), Возраст (age), Телефон (phone), and Email. The table shows 12 profiles in total.

фото	Пол	Возраст	Телефон	Email
	Ж	22		
	Ж	27		
	Ж	20		
	Ж	25		
	Ж	26		
	Ж	21		
	М	37		
	М	27		
	М	37		

Отчет об обнаруженных нарушителях

Operator

Рабочий стол

База профилей

Авторизации

Проверки присутствия

Отчеты

Хранилище отчетов

Авторизации

Контроль присутствия

Статистика по отсутствию...

Непройденные проверки

Обнаруженные нарушит...

Видео

Журналы

Справочники

Настройки

Поиск в меню

RU

Copyright 614-Logon 2023

Обнаруженные нарушители

Дата и время с:Дата и время по:ФИО:Камера:Устройство:Тип нарушения:Департамент:

Список

Фото с камеры	Фото профиля	ФИО	Дата и время	Департамент	В списках	Устройство	Камера	Тип нарушения
			02.05.2023 18:34:08			DEPLOYM-VAHLN0G	DEPLOYM-VAHLN0G	Отсутствуют неизвестные
			02.05.2023 18:29:22			DEPLOYM-VAHLN0G	DEPLOYM-VAHLN0G	Отсутствуют неизвестные
			02.05.2023 18:18:29			DEPLOYM-VAHLN0G	DEPLOYM-VAHLN0G	Отсутствуют неизвестные
			02.05.2023 18:11:50			DEPLOYM-VAHLN0G	DEPLOYM-VAHLN0G	Отсутствуют неизвестные
			02.05.2023 18:08:00			DEPLOYM-VAHLN0G	DEPLOYM-VAHLN0G	Отсутствуют неизвестные
			02.05.2023 18:06:52			DEPLOYM-VAHLN0G	DEPLOYM-VAHLN0G	Отсутствуют неизвестные
			02.05.2023 18:05:34			DEPLOYM-VAHLN0G	DEPLOYM-VAHLN0G	Отсутствуют неизвестные
			02.05.2023 17:47:49			DEPLOYM-VAHLN0G	DEPLOYM-VAHLN0G	Отсутствуют неизвестные
			02.05.2023 17:47:33			DEPLOYM-VAHLN0G	DEPLOYM-VAHLN0G	Отсутствуют неизвестные

Всего: 59

Журнал авторизации пользователей

Operator

Рабочий стол

База профилей

Авторизации

Проверки присутствия

Reports

Журналы

Мои уведомления

Дублирование профилей

Авторизации

Авторизации

Компрометации

Заблокированные устро...

Контроль присутствия

Видео

Импорт фото

Поиск в меню

RU

Copyright 614-Logon 2023

Журнал авторизаций / Авторизация от 07.07.2023 14:03:53

Общая информация

Дата и время начала:07.07.2023 14:03:00

Дата и время окончания:07.07.2023 14:04:00

ФИО:

Логин:user

Должность:

Камера:Demo-Pc

Подразделение:

Результат

Тип учетной записи:Групповая

Логин:user

Список:Employees

Тип авторизации:Операционная система

Устройство:Demo-Pc

Текущий шаг:Верификация по лицу

Пройдено шагов:2

Не пройдено шагов:0

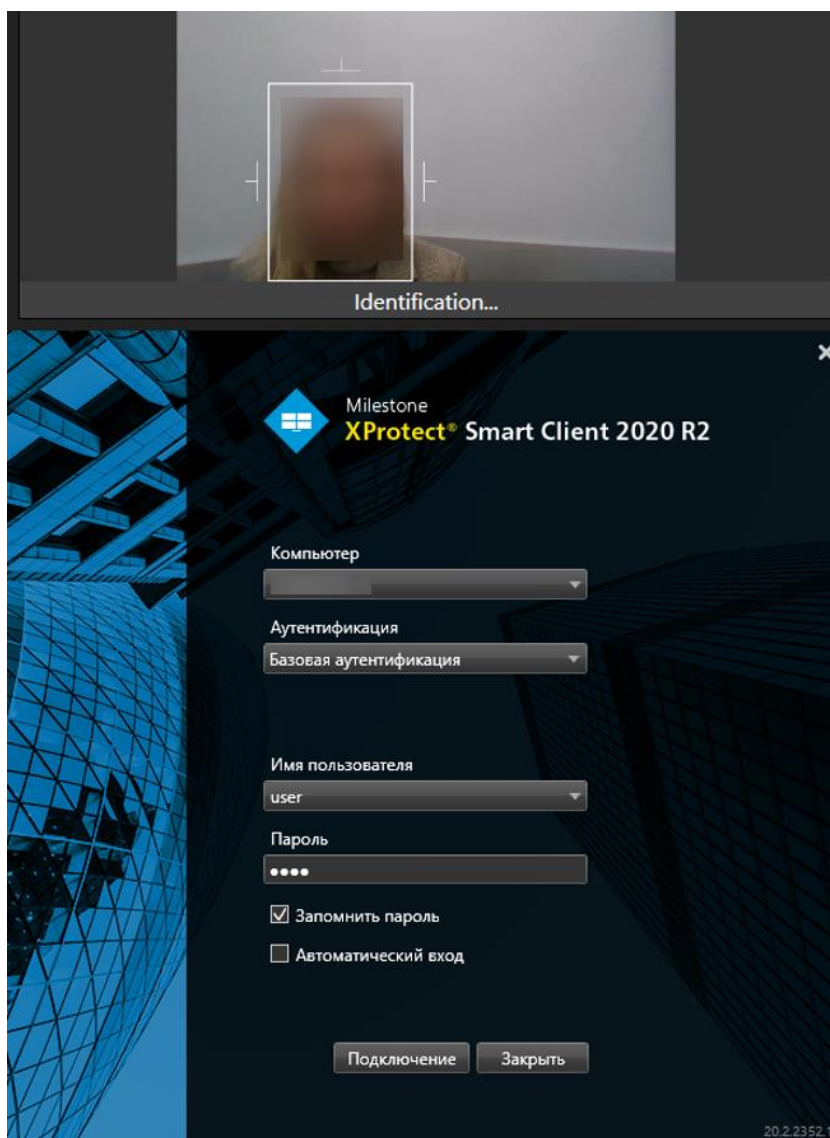
Статус:Выполнена

Фото авторизации

Фото профиля

Перейти к профилю

Id-Logon, интегрированный в интерфейс Milestone XProtect



БАНКИ И ФИНАНСОВЫЕ УЧРЕЖДЕНИЯ

ПРИМЕР ИСПОЛЬЗОВАНИЯ РЕШЕНИЯ:

Развитие технологий кибератак, значимость и чувствительность циркулирующей информации вынуждает банки внедрять новые и постоянно совершенствовать существующие системы информационной безопасности.

Постоянное расширение и совершенствование законодательных норм и стандартов в сфере банковской информационной безопасности связаны с тем, что банки осуществляют множество различных операций, ведут деятельность по разным направлениям, которые нуждаются в соответствующих инструментах обеспечения информационной безопасности.

Система Id-Logon с помощью биометрических технологий позволяет обеспечить надежную и удобную биометрическую аутентификацию сотрудников банка в корпоративных информационных системах, контролировать нахождение сотрудника банка за рабочим местом, ограничивать доступ к информационным ресурсам при отсутствии сотрудника на рабочем месте, а также подтверждать значимые операции с использованием биометрического подтверждения личности сотрудника.

- Безопасная биометрическая аутентификация сотрудников банка в различных корпоративных информационных системах
- Удобная беспарольная аутентификация с использованием биометрических данных пользователей
- Дополнительный режим двухфакторной аутентификации: биометрические данные и пин-код/пароль
- Периодическая проверка статуса пользователя, находящегося перед экраном клиентского устройства
- Выполнение различных сценариев ограничения доступа к корпоративным информационным ресурсам банка и информирование службы информационной безопасности при несоответствии статуса пользователя
- Оперативное уведомление служб информационной безопасности при работе более чем одного пользователя с клиентским устройством
- Своевременная обработка вызовов от информационных корпоративных и DLP-систем на биометрическую верификацию пользователя при совершении значимых операций или подозрении на возможную утечку информации
- Наличие готовой интеграции с Microsoft Active Directory, а также возможность интеграции с другими LDAP-каталогами, такими как: Oracle Internet Directory, IBM Tivoli Directory Server
- Возможность дополнительной проверки прихода сотрудника банка в офис организации при выполнении аутентификации в информационных системах путем взаимодействия Id-Logon с Id-Gate — программным продуктом обогащения биометрическими возможностями систем контроля доступа

ЭНЕРГЕТИКА

ПРИМЕР ИСПОЛЬЗОВАНИЯ РЕШЕНИЯ:

Энергетический комплекс принадлежит к числу стратегических отраслей, которые нуждаются в особых мерах обеспечения информационной безопасности. Если на рабочих местах в администрациях и управлениях достаточно стандартных средств информационной безопасности, то защита на технологических участках генерации энергии и доставки конечным пользователям нуждается в повышенном контроле.

Значимость информационной безопасности в энергетической сфере определяется последствиями реализации информационных киберугроз. Это не только значительный материальный ущерб и существенные репутационные издержки, но прежде всего — вред здоровью населения, нарушение инфраструктуры города или региона. Недостаточное внимание к вопросам аутентификации пользователей в корпоративных и технологических системах предприятий энергетического комплекса несет в себе дополнительные риски реализации киберугроз.

Не меньшую угрозу может представлять и отсутствие специалиста диспетчерского пункта при наступлении нештатной ситуации, которая может перерасти в полноценную аварию. Система Id-Logon с помощью биометрических технологий позволяет обеспечить надежную и удобную биометрическую аутентификацию сотрудников предприятия энергетического комплекса в корпоративных информационных системах, контролировать нахождение сотрудника за рабочим местом и информировать в случае его длительного отсутствия, ограничивать доступ к информационным ресурсам предприятия при отсутствии сотрудника на рабочем месте.

- Безопасная биометрическая аутентификация сотрудников в различных корпоративных информационных системах
- Удобная беспарольная аутентификация с использованием биометрических данных пользователей
- Дополнительный режим двухфакторной аутентификации: биометрические данные и пин-код/пароль
- Периодическая проверка статуса пользователя, находящегося перед экраном клиентского устройства
- Выполнение различных сценариев ограничения доступа к информационным ресурсам и информирование службы информационной безопасности при несоответствии статуса пользователя
- Оперативное уведомление служб информационной безопасности при работе более чем одного пользователя с клиентским устройством
- Своевременная обработка вызовов от информационных корпоративных и DLP-систем на биометрическую верификацию пользователя при совершении значимых операций или подозрении на возможную утечку информации
- Наличие готовой интеграции с Microsoft Active Directory, а также возможность интеграции с другими LDAP-каталогами, такими как: Oracle Internet Directory, IBM Tivoli Directory Server
- Возможность дополнительной проверки прихода сотрудника в офис организации при выполнении аутентификации в информационных системах путем взаимодействия Id-Logon с Id-Gate — программным продуктом обогащения биометрическими возможностями систем контроля доступа

ПРОМЫШЛЕННЫЕ ОБЪЕКТЫ

ПРИМЕР ИСПОЛЬЗОВАНИЯ РЕШЕНИЯ:

Безопасность промышленных предприятий является составной частью национальной безопасности. На промышленных предприятиях крайне важно обеспечить присутствие сотрудников на рабочих местах (центральные технологические пункты, диспетчерские пункты, посты охраны).

Отсутствие оператора или сотрудника службы безопасности на таких объектах, как атомные станции, тепловые и гидроэлектрические станции, промышленные производства, может привести к катастрофе.

Поэтому крайне важно обеспечить мониторинг нахождения сотрудника на рабочем месте.

Система Id-Logon с помощью биометрических технологий обеспечивает контроль присутствия сотрудника на рабочем месте, а также не допускает присутствия посторонних лиц.

- Безопасная биометрическая аутентификация сотрудников в различных корпоративных информационных системах
- Удобная беспарольная аутентификация с использованием биометрических данных пользователей
- Дополнительный режим двухфакторной аутентификации: биометрические данные и пин-код/пароль
- Периодическая проверка статуса пользователя, находящегося перед экраном клиентского устройства
- Выполнение различных сценариев ограничения доступа к информационным ресурсам и информирование службы информационной безопасности при несоответствии статуса пользователя
- Оперативное уведомление служб информационной безопасности при работе более чем одного пользователя с клиентским устройством
- Своевременная обработка вызовов от информационных корпоративных и DLP-систем на биометрическую верификацию пользователя при совершении значимых операций или подозрении на возможную утечку информации
- Наличие готовой интеграции с Microsoft Active Directory, а также возможность интеграции с другими LDAP-каталогами, такими как: Oracle Internet Directory, IBM Tivoli Directory Server
- Возможность дополнительной проверки прихода сотрудника в офис организации при выполнении аутентификации в информационных системах путем взаимодействия Id-Logon с Id-Gate — программным продуктом обогащения биометрическими возможностями систем контроля доступа

СХЕМА ЛИЦЕНЗИРОВАНИЯ

Id-Logon является законченным программным продуктом и распространяется посредством передачи электронных лицензионных ключей на ядро Id-Logon, а также на количество подключаемых пользователей Id-Logon.

Лицензия на пользовательские рабочие места



Лицензия на ядро Id-Logon и пользовательские рабочие места

Техническая поддержка



1. Анализ нештатных ситуаций в работе Id-Logon
2. Предоставление обновлений Id-Logon и документации
3. Консультирование по вопросам настройки и изменения конфигурации решения