

DeviceLock для соответствия закону HIPAA



Оглавление:

- [Введение](#)
- [Требования HIPAA](#)
- [Требования HIPAA Security Rule](#)
 - [Структура требований](#)
 - [Административные меры безопасности](#)
 - [Физические меры безопасности](#)
 - [Технические меры безопасности](#)
 - [Требования к хранению электронной документации](#)
 - [Выводы](#)
- [DeviceLock от Смарт Лайн Инк](#)
- [Возможности DeviceLock для HIPAA](#)
- [О компании Смарт Лайн Инк](#)
- [Контактная информация](#)

Введение

В соответствии с законом HIPAA (Health Insurance Portability and Accountability Act, Public Law 104-191) от 1996 года все американские организации, использующие в своей работе персональные медицинские сведения граждан, обязаны гарантировать конфиденциальность этой информации. Требования HIPAA обязательны для исполнения медицинскими учреждениями, фирмами, занимающимися страхованием в области здравоохранения, правительственными агентствами и другими организациями, у которых есть доступ к медицинским записям граждан.

Требования к секретности и конфиденциальности, сформулированные в HIPAA, нашли свое выражение в двух дополнительных нормативных актах. Во-первых, HIPAA Privacy Rule («[Standards for Privacy of Individually Identifiable Health Information](#)»). Этот документ требует обеспечить конфиденциальность абсолютно всех медицинских сведений, будь они в бумажном и электронном виде или даже произносятся врачом вслух. В целом, HIPAA Privacy Rule фокусируется на общих проблемах обеспечения защищенности персональных медицинских данных, например, случаях раскрытия этих сведений третьим лицам и организациям. Во-вторых, HIPAA Security Rule («[Health Insurance Reform: Security Standards](#)»). Данный стандарт содержит уже более детальные требования к защите электронных медицинских записей, описывает необходимые политики и процедуры.

За нарушение положений HIPAA предусмотрена гражданская и уголовная ответственность. Так, Министерство здравоохранения может оштрафовать нарушителя из расчета 100 долларов за одно несоответствие требованиям HIPAA. Однако если человек сознательно получает или разглашает чужие медицинские сведения в нарушение требований HIPAA, то его могут оштрафовать на 50 тыс. долларов и приговорить к лишению свободы на срок до 1 года. Для злостных нарушителей, торгующих персональными данными о здоровье граждан и противодействующих следствию, наказание может быть увеличено до 250 тыс. долларов и до 10 лет тюрьмы.

В данном документе будут рассмотрены требования HIPAA Security Rule, которые влияют на информационную инфраструктуру компаний и использующиеся в ней средства безопасности, а также возможности продукта DeviceLock компании Смарт Лайн Инк, при помощи которого организация может гораздо эффективнее достичь соответствия закону HIPAA.

Требования HIPAA

Прежде всего, следует точно определить, какие организации обязаны выполнять требования закона. Согласно формулировкам HIPAA, в его область действия попадают три типа организаций (covered entities). Во-первых, организации (health plans), предоставляющие индивидуальные или коллективные страховые полисы, в рамках которых производится оплата медицинских расходов пациента. Во-вторых, организации (health care clearinghouses), занимающиеся обработкой транзакций и трансформацией медицинской информации из одного формата в другой. Обычно эти организации служат посредниками между страховыми компаниями (health plans) и учреждениями здравоохранения (health care provider). В-третьих, в область действия HIPAA попадают сами поставщики медицинских услуг (health care provider), которым приходится работать с персональной информацией о здоровье пациентов и передавать ее по коммуникационным сетям. Отметим, что если компания все еще сомневается, попадает ли она в область действия HIPAA, то ей следует воспользоваться специальным [опросным листом](#).

Теперь посмотрим, какие категории информации подпадают под действие HIPAA. Закон защищает всю индивидуально идентифицируемую медицинскую информацию (IHI – individually identifiable health information), хранящуюся в организации, или передаваемую ее партнерам (подрядчикам, партнерам по бизнесу или аутсорсингу и т.п.). Отметим, что HIPAA защищает все данные IHI, вне зависимости от формы их представления или носителя, на котором они содержатся. Т.е. информация может быть представлена в электронном виде, на бумаге или даже произноситься вслух. Все эти сведения, защищаемые HIPAA, называются защищенной медицинской информацией (PHI – protected health information).

Более точное определение IHI – это информация, включая демографические сведения, которая относится к одному или нескольким следующим пунктам, а также нижеследующему условию.

- Сведения о прошлом, настоящем или будущем физическом или умственном состоянии здоровья человека.
- Данные о предоставлении медицинской помощи гражданину.
- Информация о прошлых, настоящих или будущих платежах за предоставление медицинской помощи субъекту.

Кроме того, чтобы эти сведения можно было отнести к IHI, они должны однозначно идентифицировать человека или представлять разумные основания, по которым можно отнести их к данному конкретному гражданину. В целом информация IHI включает довольно много обычных идентификаторов (например, имя, адрес, дата рождения, номер социального страхования и т.д.).

Требования HIPAA Security Rule

Стандарт HIPAA Security Rule оперирует таким понятием, как ePHI – то есть защищенная медицинская информация (PHI), представленная в электронном виде. Ключевое требование HIPAA Security Rule можно сформулировать следующим образом: все учреждения, хранящие или передающие медицинские данные в цифровом виде (ePHI), должны предпринимать соответствующие меры безопасности административного, технического и физического характера, чтобы:

- Обеспечить целостность и конфиденциальность ePHI;
- Отразить любые предполагаемые опасности и угрозы для ePHI;

- Предотвратить несанкционированное использование и раскрытие ePHI;
- Обеспечить общий контроль над соблюдением правил служащими и должностными лицами.

Можно сделать вывод, что HIPAA Security Rule предъявляет довольно широкие требования к безопасности ePHI. Среди них:

- **Защита от внутренних и внешних угроз.** ePHI следует защищать, как от внешних, так и от внутренних угроз.
- **Анализ рисков.** Организации должны регулярно проводить всесторонний анализ рисков.

Кроме этого, организации обязаны формально закрепить все свои политики, процессы и процедуры безопасности в письменном виде.

Структура требований

Требования HIPAA Security Rule представлены тремя категориями: административные, физические и технические меры безопасности. За этими тремя категориями скрываются 18 стандартов, из которых 12 являются спецификациями по реализации (implementation specifications). Для ясности отметим: *стандарт* определяет, что именно должна сделать организация, а *спецификация* описывает, как это должно быть сделано.

Всего в стандарт HIPAA Security Rule входят 36 спецификаций, которые удобно разделить на две группы: обязательные (required) и рекомендуемые (addressable). В первую категорию входят 14 спецификаций, а во вторую – 22 спецификации. Причем обязательные спецификации носят нормативный характер – все организации обязаны реализовать их. Что же касается рекомендуемых спецификаций, то у организаций есть три варианта действий по отношению к ним.

1. Если организация считает, что требования данной спецификации являются разумными и надлежащими, то она обязана реализовать их.
2. Если организация полагает, что требования данной спецификации не являются целесообразными и надлежащими, но достичь соответствия со всем стандартом невозможно без реализации дополнительных мер безопасности, то организация должна сделать следующее.
 - a. Обоснованно документировать, почему реализовать требования данной спецификации нецелесообразно; и
 - b. Внедрить и документировать альтернативные механизмы безопасности, которые позволяют эффективно решить ту задачу, которую призвана была решить отвергнутая спецификация.
3. Если организация посчитает, что требования данной спецификации не являются целесообразными и надлежащими, но представляется возможным достичь соответствия всему стандарту без реализации альтернативных мер безопасности, то организация должна сделать следующее.
 - a. Принять решение не внедрять данную спецификацию;
 - b. Документировать, почему реализация данной спецификации не является разумной и надлежащей; и

- с. Документировать, как будет обеспечено соответствие стандарту в этом случае.

В процессе реализации HIPAA Security Rule спецификации могут быть внедрены в любом порядке.

Административные меры безопасности

На административные меры безопасности приходится половина всех стандартов Security Rule. Эти стандарты требуют документированных политик и процедур для контроля над повседневными операциями, управления доступом служащих к ePHI, а также выбора, разработки и использования средств контроля. Далее (см. таб. 1) просуммированы стандарты, описывающие административные меры безопасности.

Таб. 1. Требования HIPAA Security Rule к административным мерам безопасности	
Требование	Расшифровка
Процесс управления безопасностью (Security Management Process)	Каждая организация должна реализовать политики и процедуры для предотвращения, выявления, исправления и документирования нарушений безопасности.
Персональная ответственность (Assigned Security Responsibility)	Каждая организация должна назначить одно лицо, которое будет нести всю ответственность за безопасность ePHI.
Внутренняя безопасность (Workforce Security)	В организации должны быть разработаны и внедрены политики, процедуры и процессы, которые гарантируют, что доступ к ePHI будут иметь только соответствующим образом авторизованный персонал.
Управление доступом (Information Access Management)	В организации должны быть разработаны и внедрены политики, процедуры и процессы, которые контролируют авторизацию, создание и изменение прав доступа к ePHI.
Тренинги (Security awareness and training)	В организации должна быть разработана и реализована программа тренингов и информирования служащих по вопросам безопасности.
Обработка инцидентов (Security incident procedures)	Каждая организация должна разработать и внедрить политики, процедуры и процессы для обработки инцидентов безопасности: ведения отчетности, принятия ответных мер и управления инцидентами.
План действия в случае непредвиденных обстоятельств (Contingency Plan)	В организации должны быть реализованы и внедрены политики, процедуры и процессы для принятия ответных мер в случае катастроф, стихийных бедствий и др. событий, которые могут вывести из строя информационные системы, содержащие ePHI.
Оценка эффективности (Evaluation)	Каждая организация должна проводить периодическую техническую и другие виды оценки эффективности политик, процедур и процессов безопасности, чтобы соответствовать требованиям Security Rule.

Безопасность партнерской сети (Business Associate Contracts and Other Arrangements)	Организации во время взаимодействия с партнерами, которые создают, получают, хранят или передают ePHI, должны разработать и использовать такие контракты, которые включают требования по реализации партнером эффективных мер защиты ePHI.
---	--

Физические меры безопасности

Физические меры безопасности – это набор требований, призванных защитить электронные информационные системы и ePHI от неавторизованного физического доступа. В целом, каждая организация, действующая в рамках HIPAA, обязана ограничить физический доступ к ePHI, сведя его только к доступу авторизованному соответствующим образом. Далее (см. таб. 2) просуммированы стандарты, описывающие физические меры безопасности:

Таб. 2. Требования HIPAA Security Rule к физическим мерам безопасности	
Требование	Расшифровка
Контроль над доступом в здание (Facility Access Controls)	Каждая организация обязана реализовать политики, процедуры и процессы, ограничивающие физический доступ к электронным информационным системам и гарантирующие доступ только в случае авторизации.
Использование рабочих станций (Workstation Use)	Должны быть разработаны и внедрены такие политики и процедуры, которые определяют надлежащее использование рабочих станций и характеристики физической среды рабочих станций, которые могут получить доступ к ePHI.
Безопасность рабочих станций (Workstation Security)	Организации должны реализовать физические меры безопасности для всех рабочих станций, имеющих доступ к ePHI, чтобы ограничить доступ к ePHI и обеспечить его только для авторизованных пользователей.
Контроль над устройствами и носителями (Device and media controls).	Каждая организация должна разработать и внедрить политики, процедуры и процессы, которые позволяют обеспечить контроль над подсоединением и отключением аппаратных устройств и электронных носителей, которые содержат ePHI. Также должен быть обеспечен контроль над перемещением этих устройств и носителей внутри организации и за ее пределами.

Технические меры безопасности

В технические меры безопасности входят несколько требований по использованию технологии для защиты ePHI. Далее (см. таб. 3) просуммированы стандарты, описывающие технические меры безопасности:

Таб. 3. Требования HIPAA Security Rule к техническим мерам безопасности	
Требование	Расшифровка
Контроль доступа (Access Control)	Организации должны разработать и внедрить политики, процедуры и процессы, которые обеспечивают доступ к информационным системам, содержащим ePHI, только тем людям и программам, которые имеют соответствующие права на это.
Средства аудита (Audit Controls)	Каждая организация должна внедрить механизмы ведения и анализа журналов действий с информационными системами, которые содержат или используют ePHI.
Целостность (Integrity)	Организации должны разработать и внедрить политики, процедуры и механизмы, защищающие ePHI от искажения (неверной модификации) или уничтожения.
Аутентификация людей и компаний (Person or Entity Authentication)	Каждая организация должна разработать и внедрить политики, процессы и процедуры, которые аутентифицируют каждого человека и каждую компанию, которые пытаются получить доступ к ePHI.
Безопасность передачи данных (Transmission Security)	Организации должны разработать и внедрить политики, процедуры и процессы, которые предотвратят неавторизованный доступ к ePHI во время передачи этих данных по электронным каналам связи, например, Интернету.

Требования к хранению электронной документации

Каждая организация, входящая в сферу действия закона HIPAA, обязана сохранять всю документацию (например, политики, процедуры и т.д.), которые должны быть разработаны в рамках Security Rule, в течение 6 лет с момента создания или вступления в силу (в зависимости от более поздней даты). Эта документация должна быть доступна для тех служащих, которые отвечают за внедрение политик и процедур. Вдобавок, организация должна периодически проверять и обновлять эту документацию, чтобы гарантировать конфиденциальность, целостность и доступность ePHI. Таким образом, процесс хранения наработанной документации и обеспечения безопасности ePHI требует непрерывных усилий организации.

Выводы

Внедрение требований HIPAA Security Rule представляет собой комплексный процесс. В первую очередь, организации требуется идентифицировать и оценить риски ePHI, а во вторую – внедрить передовой опыт, закрепленный в требованиях стандарта.

DeviceLock от Смарт Лайн Инк

Продукт DeviceLock разработан российской компанией ЗАО «Смарт Лайн Инк» и предназначен для корпоративных пользователей. С помощью DeviceLock предприятия любого масштаба могут обеспечить всесторонний контроль над информацией, покидающей корпоративную сеть через порты рабочих станций, беспроводные сети и внешние накопители. Помимо этого DeviceLock включает в себя защиту от аппаратных клавиатурных шпионов, использующихся для кражи ценной информации с рабочих станций сотрудника. Злоумышленник может подключить такое устройство между компьютером и клавиатурой служащего и тем самым обмануть антивирус и другое защитное программное обеспечение. Однако DeviceLock выявит подмену, блокирует работу «шпиона», предупредит пользователя и сделает запись в журнал событий.

Ключевой особенностью продукта является не только контроль над фактом передачи данных в соответствии с заданными политиками, но еще и полное теневое копирование всей исходящей информации. Хотя сегодня существует огромное количество решений для хранения почтовой корреспонденции, только DeviceLock позволяет собирать и анализировать информацию, покинувшую корпоративную сеть через локальные порты рабочей станции.

Когда речь заходит о контроле над карманными компьютерами, смартфонами и различными коммуникаторами, то DeviceLock не просто поддерживает теневое копирование всех данных, передаваемых на мобильное устройство, но позволяет также реализовать гибкие политики безопасности и проследить за их исполнением. Например, продукт может разрешить синхронизировать контакты и календарь, но запретить копирование файлов или синхронизацию электронной почты с вложениями.

Это крайне полезная функциональность, особенно, в свете постоянного роста популярности мобильных устройств в медицинских центрах. Кроме того, нельзя сбрасывать со счетов приближающуюся консьюмеризацию корпоративных IT-систем. Авторитетные исследовательские агентства Yankee Group и CSC Research утверждают, что директора и менеджеры IT-департаментов не могут игнорировать либо запретить то обилие портативных устройств, которыми постоянно пользуются служащие. Они просто обязаны обеспечить поддержку мобильных компьютеров сотрудников. В противном случае компания рискует потерять инновационный потенциал, снизить производительность труда своих служащих, а следом и ослабить свою конкурентоспособность. Между тем, массовая консьюмеризация чревата новыми серьезными рисками в области информационной безопасности, так как мобильные устройства могут быть использованы для осуществления мошенничества, утечки и других внутренних нарушений. Решить эту проблему, в существенной степени, позволяет DeviceLock.

Таким образом, продукт защищает компанию от утечки ePHI, попадания во внутреннюю сеть нежелательных типов данных, предоставляет инструментарий для ретроспективного анализа всей информации, которую сотрудники компании скопировали на внешние носители и забрали с собой, а также обеспечивает необходимую компании гибкость политики информационной безопасности при работе с мобильными устройствами.

Следует отметить, что DeviceLock позволяет контролировать весь спектр потенциально опасных устройств: USB-порты, дисководы, CD/DVD-приводы, а также FireWire, инфракрасные, параллельные и последовательные порты, Wi-Fi и Bluetooth-адаптеры, ленточные накопители, КПК, любые внутренние и внешние сменные накопители и жесткие диски. DeviceLock осуществляет детальный аудит действий пользователей с устройствами и данными.

Отдельно стоит выделить возможности DeviceLock по гранулированному контролю доступа пользователей к принтерам, в том числе виртуальным. Продукт не только может обеспечить выполнение политики информационной безопасности и тем самым

минимизировать риск несанкционированной утечки через принтеры, но также ведет событийное протоколирование и оставляет теньевые копии распечатываемых документов, которые впоследствии можно проанализировать и просмотреть в графическом формате.

Продукт может управляться через групповые политики Windows в домене Active Directory, благодаря чему легко интегрируется в существующую инфраструктуру организации любого масштаба.

С функциональной точки зрения DeviceLock состоит из трех частей (см. рис. 1):

1. DeviceLock Service – это агент, устанавливаемый на каждый компьютер, который автоматически запускается и обеспечивает защиту устройств на машине-клиенте, в то же время оставаясь невидимым для локального пользователя.
2. DeviceLock Enterprise Server – это дополнительный компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов аудита. DeviceLock Enterprise Server использует MS SQL Server для хранения данных.
3. Консоль управления – это интерфейс контроля, который администратор использует для управления системой, на которой установлен агент. DeviceLock поставляется с тремя различными консолями управления: DeviceLock Management Console, DeviceLock Enterprise Manager и DeviceLock Group Policy Manager.

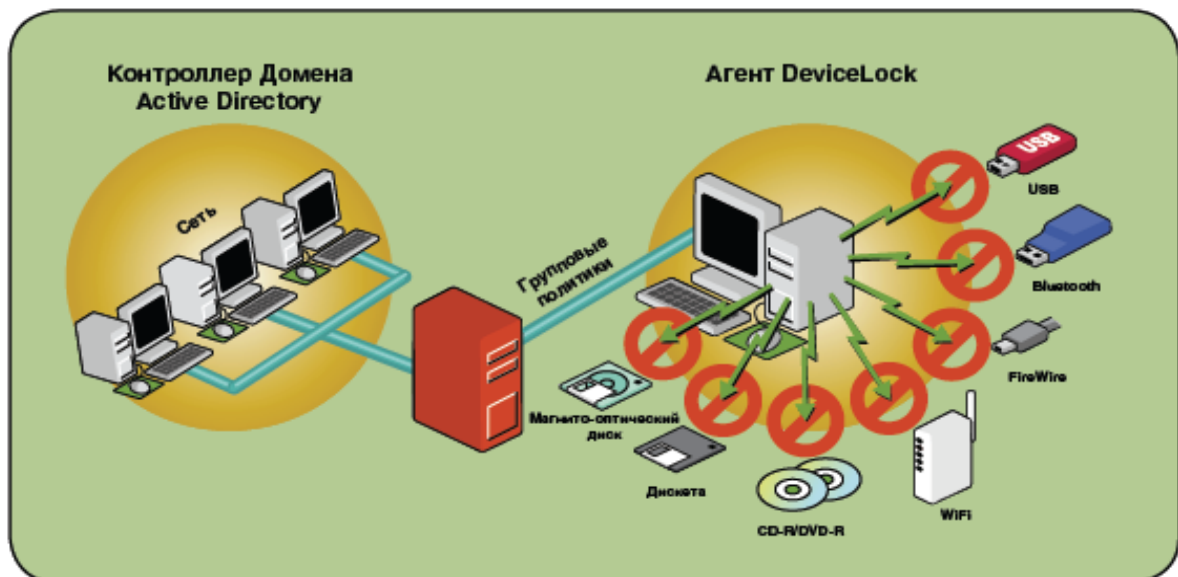


Рис. 1. Схема работы DeviceLock

Предприятия могут легко защищать десятки и сотни тысяч удаленных компьютеров при помощи DeviceLock, используя управление через групповые политики Active Directory.

Возможности DeviceLock для HIPAA

Продукт DeviceLock осуществляет контроль над передвижением данных через локальные порты рабочей станции, беспроводные сети и съемные носители на основе гибких политик. Каждый раз решение о том, чтобы разрешить или запретить доступ к внешнему устройству принимается автоматически. Таким образом, настройки и политики DeviceLock легко подвержены аудиту, а сам продукт не создает дополнительных рисков информационной безопасности.

Использование DeviceLock в корпоративной среде позволяет обеспечить соответствие двум основным требованиям HIPAA Security Rule:

- **Контроль над устройствами и носителями (Device and Media Controls).** Каждая организация должна разработать и внедрить политики, процедуры и процессы, которые позволяют обеспечить контроль над подсоединением и отключением аппаратных устройств и электронных носителей, которые содержат ePHI. Продукт DeviceLock позволяет полностью решить эту проблему.
- **Средства аудита (Audit Controls).** Каждая организация должна внедрить механизмы ведения и анализа журналов действий с информационными системами, которые содержат или используют ePHI. На помощь приходит продукт DeviceLock, отвечающий за теневое копирование всех данных на сменные носители и мобильные устройства. Анализируя собранную информацию, можно легко определить, кто, когда, каким способом и какие данные ePHI копировал во внешнюю среду.

В таблице далее (см. таб. 4) просуммирована функциональность DeviceLock в соответствии с требованиями HIPAA Security Guideline.

Таб. 4. Функциональность DeviceLock применительно к требованиям HIPAA Security Rule	
Административные меры безопасности	Возможности DeviceLock
Процесс управления безопасностью и персональная ответственность	При помощи DeviceLock руководство организации может эффективно управлять процессом передачи ePHI во внешнюю среду через локальные коммуникации рабочих станций. Использование DeviceLock позволяет гарантировать, что доступ к внешним устройствам получают только те служащие, которым это разрешено в силу политики безопасности.
Внутренняя безопасность и управление доступом	DeviceLock помогает решить проблему утечек ePHI посредством детального контроля коммуникаций через локальные интерфейсы и порты корпоративных персональных компьютеров, даже если кражу информации попытается осуществить внутренний злоумышленник. Более того, теневое копирование позволит выявить инсайдера постфактум и доказать его вину.
Контроль доступа и средства аудита	Каждая организация должна внедрить механизмы ведения и анализа журналов действий с информационными системами, которые содержат или используют ePHI. Эту задачу легко решить с помощью DeviceLock - теневое копирование данных на сменные носители и мобильные устройства позволяет легко определить, кто, когда и какие данные ePHI копировал во внешнюю среду.
Контроль над устройствами и носителями	В соответствии с HIPAA Security Rule, каждая организация должна разработать и внедрить политики, процедуры и процессы, которые позволяют обеспечить контроль над подсоединением и отключением аппаратных устройств и электронных носителей, которые содержат ePHI. Продукт DeviceLock позволяет полностью решить эту проблему, обеспечив документальное подтверждение того, кто и к каким устройствам имеет доступ.

О компании Смарт Лайн Инк

Разработчик DeviceLock – ЗАО “Смарт Лайн Инк”. Основанная в 1996 году, российская компания Смарт Лайн Инк (SmartLine Inc) занимается разработкой программного обеспечения для администрирования компьютерных сетей. Качество и надежность продуктов Смарт Лайн Инк подтверждают более 55 тысяч клиентов в 80-ти странах мира – государственные, военные, медицинские, образовательные, крупнейшие финансовые и коммерческие учреждения, а также компании малого и среднего бизнеса. Программное обеспечение Смарт Лайн Инк установлено на более чем 3 000 000 компьютерах. В число клиентов компании входят Центральный Банк РФ, Сбербанк России, ОАО "Силловые машины", ВТБ 24, Российская государственная библиотека, BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank. Смарт Лайн Инк – международная компания с офисами в Лондоне, Милане, Москве, Ратингене (Германия) и Сан Рамоне (штат Калифорния, США). Основной офис разработки программных продуктов Смарт Лайн Инк находится в Москве.

Контактная информация

ЗАО “Смарт Лайн Инк”

Москва, Б. Семеновская ул., д. 40, офис 301

Телефон: +7 (495) 967-99-60, +7 (495) 366-21-93 (контактное лицо – Анастасия Дементьева)

Отдел продаж: sales@devicelock.com

Тех. поддержка: support@devicelock.com