жёсткого диска, реестра и доступа отдельных приложений в сеть.

Намеренные же инсайдерские действия остановить традиционными системами защиты невозможно в принципе. Распределение ролей пользователей может снизить вероятность инсайдерских действий со стороны рядового персонала, но использование вредоносного кода или прав доступа более высокого уровня позволяет инсайдерам преодолевать наложенные на них ограничения. Кроме того, администратора системы не контролирует никто и ничто и, в принципе, он может сделать абсолютно всё, что захочет. Обычные антивирусы, использующиеся в медучреждениях, никогда не были приспособлены для защиты от утечки данных, а купольная защита сама по себе защищает только работоспособность системы, и необходимо использовать особые модули контроля действий приложений и сотрудников, в том числе – контроля действий администраторов и доверенных лиц. Кроме того, в данном случае высокая компьютерная грамотность работает на злоумышленника, так как в условиях, когда большинство сотрудников недостаточно представляет себе последствия тех или иных действий, инсайдерская активность может продолжаться без обнаружения на протяжении очень долгого времени. Рабочие компьютеры представляют собой малоинтересную цель для инсайдера, но базы данных, имеющиеся в МИС, – лакомая цель для кражи. Тяжёлые же устройства не защищены от инсайдерской деятельности, так как на них имеются входы для носителей информации, позволяющие инсайдеру заразить такой прибор с использованием одного flash-накопителя или диска.

Анализ рынка предоставления медицинских услуг говорит о том, что медицина в нашей стране движется к развитию частной медицины в противовес государственной. Чем более медучреждения будут заинтересованы в прибыли за счёт предоставления услуг, тем больше опасность возникновения конкурентной борьбы на рынке таких услуг. Кибератаки, способные уничтожить конкурента и не оставить следов, будут так же популярны в этой области рынка, как и в любой другой, а это значит, что незащищённая частная клиника находится в зоне постоянного риска разорения.

Персональные данные пациентов, в свою очередь, представляют ценность как с точки зрения бизнеса, так и с криминальной точки зрения. Все варианты возможных действий с такими данными перечислять бессмысленно, стоит только отметить, что в западных странах, например, в США, медицинские персональные данные уже являются одной из самых интересных целей для преступников, соревнуясь только с финансовой информацией. С очень высокой степенью вероятности инциденты потери и похищения персональных данных в медучреждениях уже происходят, и происходят относительно часто. Однако, как, например, в банковской сфере, такие инциденты замалчиваются, так как способны очень сильно повредить репутации учреждения.

Чтобы прояснить некоторые моменты, мы организовали в офисе своей компании встречу с главным врачом «Клиники экспертных медицинских технологий» Юрием Раскиным и задали ему несколько вопросов.

> К.К.: Юрий, добрый день! Скажите, пожалуйста, какие системы защиты сейчас обычно стоят на компьютерах в медучреждениях?
>
> Ю.Р.: На рабочих станциях и серверах обычно стоят антивирусные программы, настроенные на проведение регулярного сканирования системы. Это обычные антивирусные сканеры без дополнительного функционала, который сейчас встречается в некоторых решениях. Есть закон «О персональных данных», последнее изменение в который было внесено в 2011 году, и его требованиям учреждения стараются соответствовать, но на этом забота о безопасности обычно заканчивается.
>
> К. К.: Есть ли какие-то системы защиты информации от утечки по вине неосторожного сотрудника или инсайдера?
>
> Ю.Р.: Никаких подобных систем нет. Если у учреждения есть свой системный администратор, то он раздаёт роли с определёнными доступами для разных сотрудников, но это – всё. У себя я стараюсь контролировать его действия, потому что понимаю опасность утечки данных, но вот оборудование при желании такой администратор сможет вывести из строя.
>
> К.К.: Как происходит переписка между сотрудниками, между сотрудниками и пациентами? Если используется электронная почта, то используется ли собственный почтовый сервер или

сторонние ресурсы, насколько это всё защищено?
Ю.Р.: Обычно используются внешние бесплатные почтовые серверы с браузерным интерфейсом, какая уж тут безопасность?! Впрочем, в некоторых организациях этот вопрос решается. Обычно используется свой почтовый сервер и почтовый клиент, почти всегда – Outlook. Для конференций обычно используется Skype. В некоторых МИС реализованы функции переписки врачей с помощью встроенных средств, это обычно либо переписка через свой почтовый сервер, либо система мгновенного обмена сообщениями.

К.К.: Как хранятся персональные данные – исключительно в рамках МИС или же имеются отдельные документы в различных форматах, хранящиеся иначе? Если такие документы существуют и используются, есть ли какие-то системы их защиты, шифрования или контроля доступа к ним?

Ю.Р.: Сейчас нет возможности привести все документы в единый формат и читабельный электронный вид, поэтому самые разные документы просто прикрепляются к карте. Это могут быть как обычные файлы Word, так и PDF или изображения с результатами сканирования документов. Доходит до смешного – иногда при использовании тяжёлого оборудования анализы распечатывается на встроенном принтере, потом сканируются на стоящем рядом постороннем компьютере, и получившееся изображение уже используется в медицинских целях в дальнейшем. Разумеется, никаких особых систем защиты таких документов нет, в лучшем случае они просто хранятся на сетевых ресурсах с ограниченным доступом.

К.К.: Какие операционные системы стоят на тяжёлом оборудовании, всегда ли у них есть порты для внешнего доступа?

Ю.Р.: На всех приборах стоит Windows, причём, на некоторых я сам видел анимацию загрузки при включении. Операционная система по сравнению с обычными компьютерами ограничена и усечена, на неё устанавливается специализированное ПО, обеспечивающее непосредственную работу прибора. Появляющиеся в последнее время китайские варианты ничем существенно не отличаются от моделей, уже распространённых на рынках, разве что стоят дешевле и не имеют такой гарантии качества, но «начинка» у них одна. Порты доступа есть всегда – к нам, например, приезжает для обновлений сервисный инженер с флэшкой, на более старых моделях используются диски, также к приборам обычно подключён принтер.

К.К.: Юрий, спасибо за информацию.

Резюмируя всё вышесказанное, можно с уверенностью утверждать – информатизация медицины в России сейчас находится в начале пути и вопросам информационной безопасности уделяется недостаточно внимания. Частные клиники защищены лучше государственных, поскольку не просто выполняют требования действующего ФЗ-152, а проявляют инициативу в области защиты данных клиентов и дорогостоящего оборудования, но распространённого решения в данной области пока нет. Антивирус, сам по себе, не способен защитить медучреждение от всего спектра угрожающих ему кибератак, так что эффективное решение для защиты медучреждения должно вобрать в себя как сохранение работоспособности системы, так и недопущение атаки с применением вредоносного кода, не существующего в вирусных базах, и предотвращение, контроль и логирование действий собственных сотрудников как на рабочих местах, так и в базах данных и на тяжёлом оборудовании. Тяжёлое оборудование сейчас практически не защищено, что представляет особенную опасность для использующих его учреждений. Рынку необходимо решение для защиты информации, специализированное под все особенности медицинского учреждения – устаревшие компьютеры с разными версиями ОС Windows, слабые конфигурации компьютеров, тонкий канал связи машин с сетью и наличие изолированных машин, не имеющих сетевого доступа вообще. Такое решение должно либо совмещать в себе «Антивирус» и «Купол», либо быть купольным, потому что антивирусы с ситуацией не справляются.

Кирилл Кожевников, SafenSoft
для журнала «Персональные данные»