Симбиоз SIEM и DLP многократно повышает уровень информационной защиты организации и упрощает работу службе безопасности.

Литература

1. Исследование утечек конфиденциальной информации в 2016 году [Электронный ресурс] – Режим доступа: https://www.infowatch.ru/analytics. – Дата доступа: 19.05.2017.

АНАЛИЗ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОГРАММНЫХ ПРОДУКТАХ ДЛЯ ПОЛИКЛИНИК

Е.Д. Антонов, И.С. Гречко, Ю.Ю. Григорьева

Развитие компьютеризации здравоохранения [1] в Беларуси в последние годы может заметить каждый белорус, и в первую очередь, в своей поликлинике. Программные продукты (ПП) для белорусских поликлиник (ПП для поликлиник, ППдМ) разрабатывают в основном 3 минских организации: частное ЗАО «Мапсофт» [1], Белорусский центр медицинских технологий и информатизации (БелЦМТ) [3] и Объединенный институт проблем информатики (ОИПИ) [4] АН РБ. При этом доля минских поликлиник, компьютеризированных каждой организацией, имеет примерно следующий вид: «Мапсофт» – 35 %, БелЦМТ – 25 %, ОИПИ и другие – 40 %. Все ППдМ имеют примерно одинаковую структуру и решают примерно одинаковый круг задач – автоматизация деятельности врача, автоматизация структурных подразделений поликлиники (бухгалтерия, снабжение, статистика и др.).

Однако защита персональных данных пациентов в ППдМ всех разработчиков находится на уровне разграничения прав доступа к данным и контроля за доступом путем анализа логов. В условиях наличия в каждой минской поликлинике неавтоматизированной регистратуры, где хранятся бумажные амбулаторные карты пациентов, вышеописанная защита теряет смысл: зачем злоумышленнику преодолевать сложности доступа к электронным данным, когда проще получить эти данные у низкооплачиваемого работника регистратуры поликлиники. В этих условиях надежная защита персональных данных пациентов в ППдМ будет реализована только после внедрения организационных мероприятий по компьютеризации существующих в поликлиниках регистратур с бумажными амбулаторными картами пациентов.

Литература

1. Демидов, А.В. Информатизация организаций здравоохранения Республики Беларусь // Вопросы организации и информатизации здравоохранения / А.В. Демидов. – 2014. – № 3. – С. 20–25.

2. «МАПСОФТ» – разработка, внедрение и обслуживание ПО [Электронный ресурс]. – Режим доступа: www.mapsoft.by/of AWG-based WDM-PON Architecture with Multicast Capability. – Дата доступа: 19.05.2017.

3. БелЦМТ [Электронный ресурс]. – Режим доступа: www.belcmt.by/. – Дата доступа: 19.05.2017.

4. Объединенный институт проблем информатики[Электронный ресурс]. – Режим доступа: uiip.bas-net.by/. – Дата доступа: 19.05.2017.

МЕТОДИКА КАТЕГОРИЗАЦИИ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БД НА ОСНОВЕ АЛГОРИТМА КЛАСТЕРНОГО АНАЛИЗА SOM

Э.В. Артемьев

Понимание характера уязвимостей информационной безопасности имеет решающее значение для анализа угроз, которые они представляют. В значительной мере это касается таких информационных систем, как базы данных (БД), которые имеют ряд характерных особенностей, свойственных хранилищам данных: двойственная природа систем управления базами данных (СУБД), зависимость уязвимостей и механизмов управления от данных и описывающей их организацию модели, угрозы логического вывода, различная значимость сочетаний данных. Все это определяет специфический характер уязвимостей информационной безопасности БД. Поэтому для повышения эффективности защиты при выборе методов