– на 6 (30 %) из 20 КФО тип вредоносных функции уязвимых referrer-файлов детектируется явным образом как вредоносное ПО (malware, exploit, trojan);

– выявлены 7 уязвимых файлов/приложений, которые наиболее часто используются на сетевых сервисах/ресурсах ДБО КФО;

– только 9 КФО (36 %) не имеют уязвимости к реализации метода социальной инженерии (киберсквоттинг, тайпсквоттинг, фишинг).

3. Из используемых SSL-сертификатов максимальный уровень валидации (EV SSL) на основном домене КФО имеет 7 организаций (28 %).

ТЕСТИРОВАНИЕ СЕТЕВЫХ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

В.В. Маликов, А.Н. Бойко, Д.В. Калинин

Проведено статистическое исследование и тестирование уровня информационной безопасности (ИБ) сетевых систем видеонаблюдения (ССВН) по результатам которого можно сделать следующие выводы:

1. По результатам статистического исследования (опроса) по критерию близости: преимущественное использование на объектах различных категорий в Республике Беларусь, основными вендорами по ССВН в Беларуси являются: «Hikvision» (34,6 %), «Dahua Technology» (10,3 %), «Axis» (9 %).

2. Тестирование ССВН на предмет наличия уязвимостей, а также способов их эксплуатации через сетевые каналы сопряжения и коммуникации показало:

общее количество устройств ССВН (DVR, NVR, NAS и IP-камер) доступных через сеть – 2066 шт., из них 866 шт. (41,9 %) – имеют потенциальные уязвимости;

– общее количество доступных через сеть устройств ССВН (DVR, NVR, NAS и IP-камер) производителей: «Hikvision» – 34 шт. (1,7 %), «Dahua Technology» – 33 шт. (1,6 %), «Axis» – 1 шт. (0,05 %);

– как минимум 1 веб-сервер ССВН имеет заводские (по умолчанию) настройки «логин-пароль» администратора;

– показан пример успешной эксплуатации уязвимости «Heartbleed» (CVE-2014-0160) на типовой уязвимой ССВН, выявленной по результатам тестирования.

МОДУЛЬ ОБМЕНА ДАННЫМИ ДЛЯ ERP-СИСТЕМЫ MICROSOFT DYNAMICS 365 FOR OPERATIONS С ВНЕШНИМИ ПРИЛОЖЕНИЯМИ

А.С. Манин

В работе рассматривается программный модуль для интеграции ERP-системы Microsoft Dynamics 365 for Operations с внешними приложениями, такими как внешние web-сервисы и мобильные приложения. Проблемы обеспечения безопасности являются критическими для ERP-систем, так как оные используются в финансовой сфере. Кроме того, в рамках данной работы, существует необходимость обечения безопасности данных, исходящих из ERP-системы и используемых извне.

Большинство современных ERP-систем, в том числе Microsoft Dynamics 365 for Operations, адаптируют традиционную модель управления доступом на базе ролей как основное средство обеспечения безопасности в системе. Данная модель позволяет пользователям выполнять строго определенные транзакции и получать доступ к установленным бизнес-объектам [1]. Модель, представленная в ERP-системе Microsoft Dynamics 365 for Operations, не является избыточной, что обуславливает необходимость ее доработки. Для этого были созданы набор специфичных для модуля ролей, привилегий и технологических циклов – сущностей модели безопасности.

Обмен между ERP-системой и внешней средой обеспечивается средствами стандартизированнного протокола для создания и обмена данными OData [2]. Доступ к данным средствами сего протокола порождает ряд проблем безопасности, таких как пользовательский доступ к web-сервисам на базе OData на обоих конечных узлах (ERP-система и внешнее приложение). Для обеспечения постоянства доступа пользователя как внутри ERP-системы, так и во внешнем приложении, используется открытый протокол авторизации OAuth [3]: