

– на 6 (30 %) из 20 КФО тип вредоносных функции уязвимых referer-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 обеспечения 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 стандартизованного 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]:

внешнее приложение запрашивает маркер доступа в Azure Active Directory – службе управления удостоверениями и доступа ERP-системы Microsoft Dynamics 365 for Operations, который впоследствии используется для получения данных из ERP-системы.

Несмотря на использованные средства обеспечения безопасного соединения между узлами распределенной системы, использованных в работе, следует отметить возможность улучшения безопасности с использованием на стороне пользователей методов многофакторной аутентификации: биометрическая аутентификация, использование одноразовых паролей, смарт-карт и т.д.

### **Литература**

1. Петренко С.А., Курбатов В.А. Политики информационной безопасности. Москва: ДМК Пресс, 2006 400 с.

2. OData Version 4.01 Part 1: Protocol [Электронный ресурс]. – URL: <http://docs.oasis-open.org/odata/odata/v4.01/odata-v4.01-part1-protocol.html> (дата обращения: 18.05.2018).

3. The OAuth 2.0 Authorization Framework [Электронный ресурс]. – URL: <https://tools.ietf.org/html/rfc6749> (дата обращения: 18.05.2018).

## **ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ВЕРИФИКАЦИИ ЦЕЛОСТНОСТИ**

А.Ф. Марко

При работе с системами, отвечающими за безопасность людей, необходимо обеспечивать контроль над целостностью программного обеспечения данных систем в процессе эксплуатации.

Целью данной работы является разработка программного средства, обеспечивающего верификацию целостности программной части программно-аппаратной системы автоматизированного управления транспортным узлом.

На этапе проектирования программного средства был принят следующий алгоритм обеспечения целостности программной части системы:

- формирование контрольных сумм от различных категорий объектов данных и программирования с помощью алгоритма MD5;
- сохранение контрольных сумм в базу данных SQL в качестве эталонных;
- повторное формирование контрольных сумм и сравнение с эталонными.

Формирование контрольных сумм осуществляется для различных категорий объектов баз данных и файлов программы.

Контрольные суммы для процедур и функций, формируются через построчное суммирование кода, за исключением пробельных и других символов, не изменяющих функциональность программы, а также подсчета для полученного результата MD5. Для получения контрольных сумм от SQL-таблиц суммируется содержание всех ячеек и формируется MD5 от полученного результата.

Для повышения вероятности обнаружения непредвиденных изменений в системе помимо расчета контрольных сумм для объектов каждой категории в отдельности, рассчитываются контрольные суммы от всей категории в целом.

Разработка программного средства велась на языке C# с использованием среды Visual Studio. Для формирования контрольных сумм от таблиц, процедур и функций баз данных применялись процедуры, реализованные на языке структурированных запросов SQL.

По результатам разработки было получено программное решение, позволяющее при запуске системы автоматически верифицировать ее целостность.

## **ПРОГРАММИРОВАНИЕ РАСШИРЕНИЯ ИНТЕГРИРОВАННОЙ СРЕДЫ РАЗРАБОТКИ VS2017**

А.Ф. Марко, К.В. Чеушев

При работе с системами контроля версий Team Foundation Server (TFS) от компании Microsoft [1], возникает необходимость верификации номера версии при сохранении выполненной работы (check In, commit), которую осуществляет TFS, присваивая унифицированный номер (Id) каждому сохранению. Однако данная система контроля версий