Intellectual systems of information protection (ISIP) are devoted the attack detection systems. As a predictive tool ISIP use neural network (NN), the system of fuzzy logic and expert systems (ES). The scheme of attack detection includes detecting abuses and anomalies [1]. In ISPI the knowledge base of ES contains the descriptions of the classification rules according relevant user profiles and the scenarios of attack on the information system (IS). Disadvantages of ISIP on ES: system is not adaptive, its not detect always unknown attacks [1].

If NN is represented as a separate attack detection system, the analysis information for abuse during traffic processing is realized. The cases to attack are directed to security administrator. Approach is speed, since only one level of analysis is used. One of the disadvantages of the NN is the opacity of the analytical results.

The next type of detection systems includes the use of NN supplemented by ES. The sensitivity of this system increases, so the ES gets the data only about the events which were regarded as suspicious. If the NN at the expense of the training was to identify new attacks, the knowledge base of ES should be updated [1].

The use of hybrid neuro-expert systems or neuro-fuzzy systems let to reflect in the system structure the fuzzy predicate rules which are automatically adjusted during NN training. The adaptive fuzzy NN let to solve individual tasks to identify threats comparing the behavior of users with existing template system and automatically configure new rules when changing field of threats [1]. A new trend in ISPI is the use of intellectual agents (IA) working in a distributed IS and programmed for search as the invasion and anomalies [2]. The following areas of IA use in information protection are identified: research on attack detection systems (ADS); automation of search in IP (organizations, technologies, services, etc.); intellectualization of decision in DP [2].

The use of multi-agent systems for IP is discussed in work [2]. In this case it is necessary to investigate widespread attacks on the information system and the process of implementation of the attacks; investigate the existing systems of attack detection and attack detection methods; design a multi-agent structure and composition of the ADS. Its develop the structure of agent in attack detection system; work out the model for knowledge representation of agents about the state of information system; develop the method of joint analysis by agents of the information system state. The multi-agent architecture ADS involves many interacting intelligent agents. The standard IS components, sources of information to be analyzed for attack detection are proposed. The structure of agents, which includes modules: management, receiving and processing data, analysis, training, response, generate messages, making a decision. The function of modules are describes. Methods of work with a multi-agent ADS includes steps; placement agents by blocks of IS; data collection, the formation of training set, attack detection, and reporting it to the administrator.

**References**

1. *Kalach A.V., Nemptina E.S.* // Internet magazine «Technology tehnosfera security» (http://ipb.mos.ru/ttb). № 3. 2011. P. 3–11.

2. *Nikishova A.V.* Izvestia JuFU. Technical science. Theme issue. «Information security» — Taganrog: TTU, JuFU. 2012. № 12 (137). P. 28–33.

## ОБЗОР И АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

В.А.ВИШНЯКОВ, ХРАЙБА МОХАММЕД

В докладе представлены результаты анализа применения средств защиты информации в электронной коммерции (ЭК). Выделены следующие направления: угрозы и технологии их предотвращения, действия по защите в ЭК, услуги защиты для ЭК, две технологии шифрования (симметричная и асимметричная), использование

брэндмауэров, технология цифровой подписи, защищенные протоколы: Secure HTTP (S–HTTP), Secure Sockets Layer (SSL), Secure Electronic Transaction (SET).

Угроза информации: данные преднамеренно перехватываются, читаются или изменяются; пользователи идентифицируют себя неправильно (с мошенническими целями); пользователь получает несанкционированный доступ из одной сети в другую. Действия по защите. Шифрование данных, препятствующее их прочтению или искажению; проверка подлинности отправителя и получателя осуществляется технологией цифровой подписи, фильтрация трафика, поступающего в сеть или на сервер защищается брэндмауэрами. Криптографические технологии обеспечивают три основных типа услуг для электронной коммерции: аутентификацию (которая включает идентификацию), невозможность отказа от совершенного и сохранение тайны.

Технология ЦП. При помощи хеш–функции получается дайджест — уникальным образом сжатый вариант исходного текста. Дайджест шифруется с помощью личного ключа и превращается в цифровую подпись, которая посылается вместе с самим сообщением.

Некоторые стандарты защиты данных для ЭК включают защищенные протоколы: S–HTTP (защищенный HTTP), SSL (является составной частью всех известных браузеров и Веб–серверов.), SET (используется для операций с кредитными карточками.).

## МОНИТОРИНГ МЕСТОПОЛОЖЕНИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ИХ АКТИВНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

Д.И. ЖУКОВСКИЙ

Мы живем во время стремительно развивающихся технологий. Вместе с повышением доступности персональных компьютеров, ноутбуков и мобильных телефонов, а также улучшения качества интернета социальные сети становятся неотъемлемой частью жизни современного человека.

Ежедневно пользователи социальных сетей публикуют большое количество различного контента, среди которого комментарии, заметки, фотографии и др. Проблема в том, что зачастую вся эта информация находится в свободном доступе и посторонний человек может узнать место, где находился пользователь в момент публикации контента. Данные о геолокации могут быть явно связаны с контентом (foursquare, twitter) или получены неявно, например на основе EXIF метаданных (vk.com, facebook).

EXIF (Exchangeable Image File Format) — стандарт, позволяющий добавлять к изображениям и прочим медиафайлам дополнительную информацию (метаданные), комментирующую этот файл, описывающий условия и способы его получения, авторство и т.д. EXIF метаданные добавляются на фотографии и видео большинством современных фотоаппаратов и телефонов.

Собирая и анализируя геолокационные данные пользователей социальных сетей можно, например, выяснить, какие места являются наиболее живописными в туристических районах, или где именно можно встретить определенного человека в различные промежутки времени в будни и выходные. С кем пересекается или общается конкретный пользователь. Если взять весь контент определенного пользователя, публикуемый им, скажем после 21:00 и до 07:00, нанести на тепловую карту, то с большой вероятностью можно определить, где именно он проживает.

Показательный пример — 20.03.2012 г. ФБР арестовало хакера Higinio O. Ochoa III, ему были предъявлены обвинения во взломе государственных сайтов и выкладывании в сеть телефонов и домашних адресов сотрудников полиции. Выйти на хакера помогла фотография, которую он разместил на странице с украденными данными. Фотография содержала EXIF метаданные с GPS координатами места, где она была сделана.