УДК 681.3

О ПРОБЛЕМАХ ЗАЩИТЫ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

© 2021 Ю. П. Преображенский, О. Н. Чопоров, Е. Ружицкий

Воронежский институт высоких технологий (Воронеж, Россия)
Воронежский государственный технический университет (Воронеж, Россия)
Панъевропейский университет (Братислава, Словакия)

В данной работе предлагается методика формализации уровней защиты различных объектов в информационных системах.

Ключевые слова: защита информации, алгоритм, информационная система.

В настоящее время проблема защиты информации в информационных системах является очень актуальной [1, 2]. Для ее решения на практике исследователями разрабатываются различные методики и подходы. В данной работе предлагается методика, позволяющая осуществлять формализацию исследуемых объектов, подлежащих защите, на разных уровнях.

Чтобы провести оценку уровня защиты пользователей некоторой информационной системы, необходимо взять в расчет некоторые объекты и их связи. Например, критичные документы и их уровень критичности для компании; связи между пользователями с доступом к критичным документам и к хостам на которых они хранятся; хосты, с которых возможно получение доступа к документам; связи между хостами; зоны которые контролируются посредством связей между пользователями; потенциальные зоны уязвимости в системе.

Помимо внутренней информации о системе необходимо учитывать, к примеру, уровень компетенции преступника, старающегося получить данные, а также его уровень осведомленности о принципе работы системы, его технологических возможностях, а также его возможные цели и методы [3].

Рассмотрим более подробно все описанные объекты. Для этого необходимо сформулировать несколько общих алгебраических моделей. Это позволит предоставить параметры, необходимые для учета при оценивании уровня защиты пользователей ИС от социоинженерных атак. Помимо этого, формулировка алгебраических моделей необходима, чтобы оценить саму вероятность кражи или поражения критичных документов.

В модель критичных документов входят элементы, связанные с уровнем критичности для компании, месторасположения на хосте критичных документов и уровней доступов к ним. Уровень финансовых потерь в случае утери документа является выражением уровня критичности документа. Помимо финансовых потерь, компания может понести репутационные убытки, или какие-либо другие. Эти показатели также могут нести оценку уровню критичности документа [4].

Предлагается применять систему уровней критичности документа, как вариант для построения модели. Самые критичные документы будут относиться к группе 1, менее критичные, соответственно, к группе 2, и так далее, по уровню критичности [5].

Доступ к документу может осуществляться с различных хостов, а также обладать разноуровневым доступом с хоста. Например, документ может быть доступен только для чтения с одного хоста, а с другого он может иметь доступ и для чтения, и для редактирования [6, 7]. Каждый пользователь также может иметь различные уровни доступа и ограничений. Принимая во внимание изложенное, формальную алгебраическую модель возможно представить как:

$$CD_i = \left(Lc^i ; \left\{ H_j^i \right\}_{j=1}^n ; \left\{ \left(U_k^i ; LAD_k^i \right) \right\}_{k=1}^m \right), \quad (1)$$

где Lc^i – уровень критичности документа;

$\left\{ H_j^i \right\}_{j=1}^n$ – хосты, с которых возможно получить доступ к документу;

Преображенский Юрий Петрович – Воронежский институт высоких технологий, канд. техн. наук, профессор, Petrovich@vivt.ru.
Чопоров Олег Николаевич – Воронежский государственный технический университет, профессор, chop-orov_oleg@mail.ru.
Ружицкий Евгений – Панъевропейский университет, канд. техн. наук, доцент, rush_evg_br53@yandex.ru.

$\left\{\left(U_k^i; LAD_k^i\right)\right\}$ – пользователи, у которых есть возможность доступа к документу некоторого уровня;

LAD_k^i – уровень доступа документа.

В модель хостов информационной системы входят компоненты, непосредственно связанные с программным обеспечением, установленным на хост и с пользователями, имеющими разный уровень доступа, в частности, имеющими возможность изменять конфигурацию системы, или устанавливать и удалять приложения и ПО. Кроме этого, в нее входят связи между информационной системой и хостами, а также, критичные документы, к которым можно получить доступ посредством этих связей, или иными путями.

Разными уровнями критичности могут обладать не только документы, но и хосты, что связано с уровнями критичности документов, расположенных на нем. Представить формальную модель хоста возможно в следующем виде:

$$H_i = \left(\left\{Soft_j^i\right\}_{j=1}^n; \left\{CD_t^i\right\}_{t=1}^r; \left\{Conn_k^i\right\}_{k=1}^m; \left\{\left(U_l^i; LAH_l^i\right)\right\}_{l=1}^q; Lc^i\right), \quad (2)$$

где $\left\{Soft_j^i\right\}_{j=1}^n$ – установленное на хосте ПО;

$\left\{CD_t^i\right\}_{t=1}^r$ – критичные документы, к которым можно получить доступ с хоста;

$\left\{Conn_k^i\right\}_{k=1}^m$ – связи между хостами в информационной системе;

$\left\{\left(U_l^i; LAH_l^i\right)\right\}_{l=1}^q$ – пользователи, имеющие некоторый уровень доступа к хосту;

Lc^i – уровень критичности хоста, имеющий потенциальную зависимость от уровня критичности документов, доступных с этого хоста.

Представить формальную алгебраическую модель пользователя информационной системы возможно при учете ее связи с профилем пользовательской уязвимости. Он являет собой некоторое количество пар, состоящих из уязвимости и ее выраженности. Пользовательской уязвимостью может стать уровень доступа пользователя к критичным документам и хостам; зоны, в которых пользователь имеет доступ и контроль. Помимо этого, пользователь и сам может быть уязвимым. Человеческий фактор, например, внутреннее состояние пользователя зависит от внешних факторов, таких как отношения с коллегами или семьей, конфликт с руководством, или ухудшение здоровья. Исходя из этого можно формализовать в следующем виде:

$$U_i = \left(\begin{array}{l} \left\{V_j, D_i, \left(V_j\right)\right\}_{j=1}^n; \left\{\left(AH_l^i; LAH_l^i\right)\right\}_{l=1}^m; \\ \left\{\left(AD_k^i LAD_k^i\right)\right\}_{k=1}^q; \left\{Comm_t^i\right\}_{t=1}^r; \left\{CA_a^i\right\}_{a=1}^b; State^i \end{array}\right), \quad (3)$$

где $\left\{V_j, D_i, \left(V_j\right)\right\}_{j=1}^n$ — профиль уязвимостей пользователя, где V_j – уязвимость пользователя, а $\left(V_j\right), D$ —значение уровня уязвимости V_j;

$\left\{\left(AH_l^i; LAH_l^i\right)\right\}_{l=1}^m$ – уровень доступа к хостам;

$\left\{\left(AD_k^i LAD_k^i\right)\right\}_{k=1}^q$ – уровень доступа к документам;

$\left\{Comm_t^i\right\}_{t=1}^r$ – вид корреляции между пользователями в информационной системе,

$\left\{CA_a^i\right\}_{a=1}^b$ – зоны доступные для контроля пользователя;

$State^i$ – внутреннее состояние пользователя, имеющее потенциал к влиянию на предпринимаемые пользователем действия в условиях социоинженерной атаки.

В алгебраическую модель злоумышленника входят такие компоненты, которые находятся в непосредственной связи с его профилем компетенции [8, 9].

Это некоторое количество пар видов атакующего действия и способности злоумышленника к их применению. Сюда можно отнести такие средства как исходные данные, имеющиеся у злоумышленника об информационной системе, финансы, временные интервалы, наличие сообщников, что должно быть учтено в модели.

Помимо этого, не менее важна цель злоумышленника. Это может быть вынуждение пользователя к некоторому действию, связь с конкретным пользователем или получение доступа к критичным документам. Учитывая все эти факторы формализовать

модель злоумышленника можно следующим образом:

$$M_i = \left(\left\{\left(R_j, Q_i, \left(R_j\right)\right)\right\}_{j=1}^{n}; \left\{\left(A_k, S_i\left(A_k\right)\right)\right\}_{k=1}^{m}; \left\{BK_l^i\right\}_{l=1}^{q}; G^i; \left\{Comm_t^i\right\}_{t=1}^{r}\right), \quad (4)$$

где $\left\{\left(R_j, Q_i, \left(R_j\right)\right)\right\}$ – доступные для злоумышленника средства;

$\left\{\left(A_k, S_i\left(A_k\right)\right)\right\}_{k=1}^{m}$ – профиль компетенций злоумышленника;

$\left\{BK_l^i\right\}_{l=1}^{q}$ – исходные данные, имеющиеся у злоумышленника об информационной системе;

G^i – достигаемая злоумышленником цель;

$\left\{Comm_t^i\right\}_{t=1}^{r}$ – потенциальные связи между злоумышленниками.

Нами были проанализированы модели, которые были адаптированы к задачам сущностей, речь о которых шла ранее. Это позволит не производить решение исследованных ранее в [10-12] задач.

Тем не менее, в условиях более развернутых исследований, существует вероятность дополнения моделей неучтенными компонентами, способными влиять на оценку защищенности пользователей и оценку вероятности поражения критичных документов социоинженерными атаками.

Помимо этого, возможно изменение оценки уровня защиты пользователей и уровня их поражаемости. Это может произойти, например, если сотрудники компании проходили обучение по части информационной безопасности, тогда вероятность успешного осуществления атаки будет меньше. Такое обучение может включать в себя разъяснения о потенциальных социоинженерных угрозах, способы противостояния атакам, и прочую информацию, способную помочь в отражении атак.

Пусть $p(0)$ – посттренинговая вероятность успеха социоинженерной атаки злоумышленника на пользователя, примем ее обозначение как $p_0 = p(0)$. Нужно отметить, что $p_0 \in [0;1]$.

В таком случае в течение некоторого времени возможно изменение вероятности поражения пользователя атакой злоумышленника в сторону увеличения. Это может происходить по причине уменьшения бдительности пользователя, утраты им навыков защиты, знаний или умений. Взяв за основу вышеописанную модель, становится возможно создать дифференциальное уравнение $\frac{dp}{dt} = -\alpha p$. Если исходное условие $p(0) = p_0$., вычисление p произведем следующим образом:

$$\frac{dp}{p} = -adt; \int \frac{dp}{p} = \int -adt; \ln p = -ap + C; p = Ke^{-at}; p_0 = K; p = p_0 e^{-at}. \quad (5)$$

Таким образом, представленный методический подход по формализации объектов в информационных системах, с точки зрения их защищенности, может быть полезен в различных практических приложениях.

ЛИТЕРАТУРА

1. Потудинский А. В. Модели для определения моментов контроля в многоуровневых организационных системах / А. В. Потудинский, А. П. Преображенский // Моделирование, оптимизация и информационные технологии. – 2020. –Т. 8. – № 2 (29). – С. 28-29.

2. Горбенко О. Н. О подходах для управления корпоративными ресурсами / О. Н. Горбенко, С. Ю. Черников, Я. А. Мишин // Моделирование, оптимизация и информационные технологии. – 2014. – № 3 (6). – С. 11.

3. Шаповалов А. В. Возможности применения методов оптимизации в управлении портфелями проектов / А. В. Шаповалов, А. П. Преображенский, О. Н. Чопоров // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8. – № 1 (28). – С. 32-33.

4. Lvovich I. Ya. Modeling of control process of industrial organizations based on rating approach / I. Ya. Lvovich, Ya. E. Lvovich, A. P. Preobrazhenskiy, Yu. P. Preobrazhenskiy, O. N. Choporov // Modeling, Optimization and Information Technology. – 2020. – Т. 8. – № 3 (30). – С. 34-35.

5. Потудинский А. В. Модели оптимизации «стоимость-надежность» для обслуживающих социально-экономических систем / А. В. Потудинский, А. П. Преображенский // Системы управления и информа-

ционные технологии. – 2020. – № 2 (80). – С. 14-20.

6. Львович Я. Е. Адаптивное управление марковскими процессами в конфликтной ситуации / Я. Е. Львович, Ю. П. Преображенский, Р. Ю. Паневин // Вестник Воронежского государственного технического университета. – 2008. – Т. 4. – № 11. – С. 170-171.

7. Свиридов В. И. Лингвистическое обеспечение автоматизированных систем управления и взаимодействие пользователя с компьютером / В. И. Свиридов, Е. И. Чопорова, Е. В. Свиридова // Моделирование, оптимизация и информационные технологии. – 2019. –Т. 7. – № 1 (24). – С. 430-438.

8. Горячко В. В. Характеризация географически связанных организационных систем и подход к интеллектуализации управления ими / В. В. Горячко, Э. М. Львович // Моделирование, оптимизация и информационные технологии. – 2019. – Т. 7. – № 3 (26). – С. 25.

9. Альтварг М. С. Использование принципов организационной культуры для повышения эффективности работы предприятия / М. С. Альтварг, Э. М. Львович, В. Н. Фролов // Интеллектуальные информационные системы. Труды всероссийской конференции. – 1999. – С. 26.

10. Степанчук А. П. Применение информационных технологий в организациях / А. П. Степанчук // Молодежь и системная модернизация страны. Сборник научных статей 2-й Международной научной Конференции студентов и молодых ученых. В 4-х томах. Ответственный редактор А. А. Горохов. – 2017. – С. 193-197.

11. Преображенский Ю. П. О возможностях роста эффективности функционирования современных компаний / Ю. П. Преображенский // Актуальные проблемы развития хозяйствующих субъектов, территорий и систем регионального и муниципального управления. Материалы XIII международной научно-практической конференции. Под редакцией Ю. В. Вертаковой. – 2018. – С. 215-218.

12. Кострова В. Н. Применение технологий автоматизации для повышения эффективности работы компаний / В. Н. Кострова, Т. А. Цепковская // Современные проблемы экономики и менеджмента. Материалы международной научно-практической конференции: выпуск сборника посвящен 100-летию МОТ, 100-летию ВГУ. ФГБОУ ВО «Воронежский государственный университет»; АНОО ВПО «Воронежский институт высоких технологий», Воронежское региональное отделение «Академия труда и занятости». – 2017. – С. 200-203.

ABOUT PROBLEMS OF DATA PROTECTION IN INFORMATION SYSTEMS

© 2021 Yu. P. Preobrazhenskiy, O. N. Choporov, E. Ruzhicky

Voronezh Institute of High Technologies (Voronezh, Russia)
Voronezh State Technical University (Voronezh, Russia)
Pan-European University (Bratislava, Slovakia)

This paper proposes a technique for formalizing the levels of protection of various objects in information systems.

Keywords: information security, algorithm, information system.