СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2020. – № 1–2 (97).** – 89–98

УДК 007.51 DOI: 10.17212/2307-6879-2020-1-2-89-98

МОДЕЛЬ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ СОЦИОТЕХНИЧЕСКОЙ СИСТЕМЫ НА ОСНОВЕ ПОВЕДЕНЧЕСКИХ ОСОБЕННОСТЕЙ ЧЕЛОВЕКА*

О.Г. КОРГАНОВА[1], И.Е. ПАНФИЛОВА[2]

[1] *443100, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, кандидат технических наук, доцент кафедры информационно-измерительной техники. E-mail: annuin@mail.ru*
[2] *443100, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, магистрант кафедры вычислительной техники. E-mail: panfilova_2015@bk.ru*

Сложности, связанные с описанием и прогнозированием поведения человека и его присутствием в социотехнических системах (СТС), приводят к возникновению целого ряда специфических задач, связанных с обеспечением информационной безопасности СТС и ее целостности. В статье анализируются общие и специфические угрозы информационной безопасности, возникающие в СТС, рассматриваются особенности функционирования социотехнических систем, а также приводится логика построения системы управления информационными рисками, внедряемой в структуру СТС и учитывающей поведенческие особенности человека (функцию целеполагания), для обеспечения безопасности информационных процессов в СТС.

Ключевые слова: информационная безопасность, анализ поведения, социотехническая система, информационные процессы, анализ угроз

ВВЕДЕНИЕ

Разработка и реализация различных подходов к обеспечению корректного и защищенного функционирования сложных систем была и до сих пор остается актуальной задачей. В наши дни особое место среди большого многообразия сложных систем занимают социотехнические системы (СТС), представ-

* Статья получена 15 мая 2020 г.

ляющие собой совокупность информационно-технической и социальной подсистем, а также внешней среды. Само название показывает, что в этих системах происходит взаимодействие человека (антропогенная составляющая) и машины (техническая составляющая). В связи с этим на первый план при проектировании таких систем выходит эффективное взаимодействие технологической составляющей и человеческого фактора, а также обеспечение безопасности протекающих внутри СТС информационных процессов (ИП), что является одной из самых актуальных задач в настоящее время.

1. СОЦИОТЕХНИЧЕСКИЕ СИСТЕМЫ: ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ

Основной целью создания СТС является продуктивное взаимодействие человека (антропогенной подсистемы) и технической подсистемы. Структура такой системы представлена на рис. 1 [5].

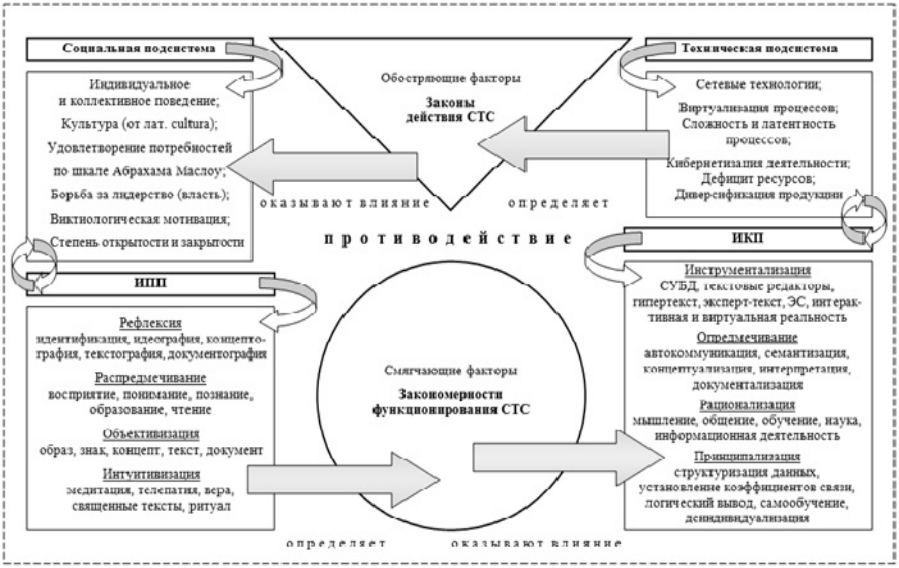

Рис. 1. Обобщенная структура социотехнической системы

Техническая подсистема представляет собой совокупность программного обеспечения, аппаратных устройств, методов, конфигураций и процедур,

применяемых пользователями системы для преобразования входных данных в выходные.

Социальная подсистема включает в свой состав людей и организации, которые взаимодействуют с системой. При этом неизбежно проявляются их уникальные социальные признаки [4].

Однако стоит отметить, что особое место в специфике функционирования СТС занимает не столько общность людей, сколько отдельно взятый человек, обладающий характерными для группы характеристиками, но в то же время являющийся независимой единицей (агентом) системы социотехнического типа.

Именно наличие такой независимой антропогенной составляющей приводит к тому, что целый ряд характеристик СТС перестают быть строго определенными: связи между элементами системы описываются нечетко; тяжело определить, что может повлиять на поведение человека как элемента такой системы; труднопредсказуем эффект влияния управляющих воздействий на антропогенные элементы системы и т. д. [6].

2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СОЦИОТЕХНИЧЕСКИХ СИСТЕМ

Для социотехнической системы, как и для любой другой сложной информационной системы, характерен ряд классических угроз, осуществимых без учета поведения внутреннего пользователя и поступающих, как правило, из внешней среды [1]. К таким угрозам можно отнести следующие:

- атаки из внешней сети (например, Интернета), направленные на искажение, уничтожение, хищение информации или приводящие к отказу в обслуживании информационных систем предприятия;
- распространение вредоносного программного обеспечения;
- нежелательные рассылки (спам);
- воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения в информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем;
- перехват информации с использованием радиоприемных устройств;
- воздействие на информацию, осуществляемое путем несанкционированного использования сетей инженерных коммуникаций;
- воздействие на персонал предприятия с целью получения конфиденциальной информации.

Однако наибольшую опасность для социотехнических систем представляют угрозы, исходящие «изнутри» системы. Такие угрозы осуществляются исходя из технических возможностей системы и инициируются самими пользователями.

17 апреля 2020 года экспертно-аналитический центр группы компаний InfoWatch сообщил результаты сравнительного исследования утечек информации, произошедших по вине или неосторожности персонала коммерческих компаний за период с 2013 по 2019 год. В 2019 году по вине внутренних нарушителей (рядовых сотрудников, руководителей, системных администраторов) произошло 53,7 % всех утечек, зарегистрированных экспертно-аналитическим центром ГК InfoWatch.

При этом важно отметить, что осуществление инсайдерских угроз не всегда является преднамеренным действием, иногда они становятся результатом некомпетентности сотрудников или случайности.

Среди наиболее популярных подходов к обеспечению безопасности СТС, учитывающих человеческий фактор, можно выделить так называемые UEBA-системы (Userand Entity Behavior Analytics). Рассмотрим основные свойства данного решения, его достоинства и недостатки.

3. ОСОБЕННОСТИ РАБОТЫ СОВРЕМЕННЫХ СИСТЕМ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ

Поведенческая аналитика пользователей и сущностей (UEBA) – это система, которая использует поведенческий анализ для мониторинга действий пользователей и инфраструктурных объектов, таких как серверы и приложения. Системы UEBA устанавливают базовый уровень активности пользователей и их взаимодействия с различными объектами, отслеживая их на предмет отклонений от этого базового уровня. Когда система UEBA обнаруживает аномалию в поведении, она отправляет оповещения сотрудникам службы безопасности, которые могут продолжить расследование. К преимуществам систем UEBA относятся:

– способность точно обнаруживать скомпрометированные учетные записи пользователей путем выявления ненормального поведения;

– системы UEBA полезны как часть программного пакета для предотвращения потери данных;

– предотвращение неправомерного использования привилегированного доступа к учетной записи путем обеспечения надлежащего использования прав доступа;

– повышение эффективности информационной безопасности благодаря автоматизации;

– уменьшенная поверхность атаки с использованием расширенной поведенческой аналитики для частого обновления информации о потенциальных слабых местах в сети сотрудниками службы безопасности.

Однако существенными недостатками подобных систем являются:

– необходимость получения большого объема данных и оперирования ими для построения нормального поведения пользователя и дальнейшего прогнозирования поведения;

– в период накопления данных UEBA может происходить структурная реорганизация, и определение стабильного характера поведения пользователей может быть затруднено, а для каких-то – невозможно. В данном случае придется дождаться, пока внутренние процессы системы придут в равновесие, и уже после этого прибегать к использованию UEBA;

– не все решения UEBA наделены возможностью динамически подстраиваться под изменяющееся поведение пользователей (люди меняются) [3].

В связи с указанными особенностями функционирования систем поведенческой аналитики авторами статьи предлагается иная логика построения информационной системы, обеспечивающей безопасность СТС на основе анализа поведенческих особенностей человека как субъекта такой системы.

4. МОДЕЛЬ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ НА ОСНОВЕ СВОЙСТВА ЦЕЛЕПОЛАГАНИЯ ЧЕЛОВЕКА

При определении цели функционирования СТС можно определить ее на начальном этапе проектирования и не изменять на всем периоде функционирования системы, а можно видоизменять цель при изменении условий окружающей среды и требований к системе. Такая вариативность усложняет задачу описания подобных систем и составление прогнозов их функционирования. Однако необходимо учитывать, что у человека, являющегося частью такой системы, в поведении есть важная особенность – *целенаправленность* его поведения, и именно наличие этой особенности может позволить всё же прогнозировать поведение системы и определять ее результативность.

Признаками наличия целенаправленности в действиях человека являются использование им операций классификации и обобщения, категоризация

полученных промежуточных или конечных результатов деятельности, определение значимости каждого из полученных результатов и его ценности для каждого конкретного пользователя в каждый конкретный момент времени [7].

При этом субъекты системы могут быть подразделены на активные и пассивные. К активным необходимо отнести такие субъекты, которые могут для всех систем или ее отдельных подсистем формировать цели и определять способы их достижения. К пассивным будем относить субъекты, не имеющие таких возможностей.

Учитывая всё вышеизложенное, необходимо отметить, что важной специфической особенностью социотехнических систем является возможность передачи управляющих воздействий от человека информационным процессам. В общем случае при проектировании и в начале функционирования такой системы активная роль закреплена за человеком, но затем в процессе функционирования она может быть переадресована информационным процессам с сохранением задач целеполагания у человека с возможностью изменения ранее поставленных целей.

Если рассматривать угрозы (или деструктивные процессы, вредоносные воздействия) информационным объектам, возникающие и действующие в таких системах, то все они проявляются и начинают функционировать как пассивные объекты, но затем возможно присвоение им активной роли и переход в статус активных субъектов системы. При этом они не обладают возможностями собственного целеполагания и их действия направлены на достижение результата, заданного конечным пользователем (человеком). Именно эти признаки – наличие значимого для конечного пользователя результата и отсутствие возможностей для определения собственных целей – и являются основанием, определяющим порядок действий и тот информационный объект, на который направлены вредоносные воздействия, формирующиеся в социотехнических системах.

Таким образом, учет таких особенностей поведения человека, как наличие конечной цели в его деятельности, а также возможный обмен ролями с информационными процессами, позволяет построить систему управлении информационными рисками, которая будет осуществлять постоянный контроль и мониторинг действий пользователя и оценку полученных им результатов. При этом одновременно необходимо осуществлять сравнительный анализ действий различных пользователей, это позволит оценить значимость достигнутых результатов для каждого из них. Общая структурная схема такой системы приведена на рис. 2.

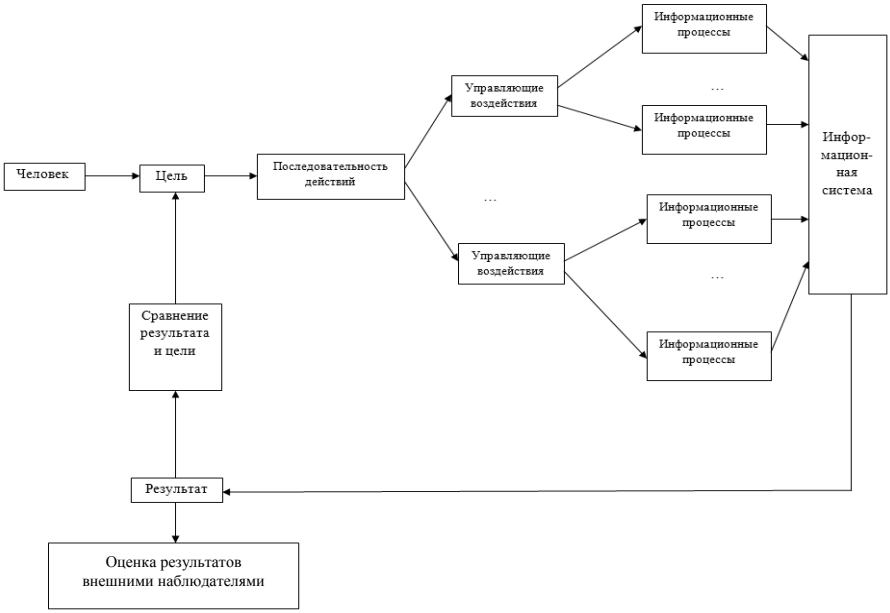

Рис. 2. Структурная схема системы управления информационными рисками

Подобная схема показана применительно к одному пользователю системы, но она может быть использована по отношению к нескольким пользователям. В таком случае в систему необходимо добавить блок сравнения целей и результатов пользователей между собой.

ЗАКЛЮЧЕНИЕ

Таким образом, в приведенной статье рассмотрен подход к построению систем управления информационными рисками, который позволяет учитывать возможность передачи управляющих воздействий от человека к информационным процессам, что является новым подходом в вопросах анализа информационных процессов в социотехнических системах.

СПИСОК ЛИТЕРАТУРЫ

1. *Васильков А.В., Васильков А.А., Васильков И.А.* Информационные системы и безопасность: учебное пособие. – М.: Форум, 2013. – 528 с.

2. *Запечников С.В.* Информационная безопасность открытых систем. В 2 т. – М.: ГЛТ, 2018. – 2 т.

3. Как системы безопасности анализируют поведение пользователей. – URL: https://clck.ru/Nctid (дата обращения: 08.07.2020).

4. *Кравченко С.И.* Безопасность социотехнических систем // НБИ Технологии. – 2018. – Т. 12, № 2. – С. 20–24.

5. *Остапенко Г.А., Мешкова Е.А.* Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия: учебное пособие / под ред. Ю.Н. Лаврухина. – М.: Горячая линия-Телеком, 2007. – 295 с.

6. *Green D.* Socio-technical systems in global markets. – 2010. – 23 August. – URL: http://nuleadership.wordpress.com/2010/08/23/socio-technical-systems-in-global-markets/ (accessed: 08.07.2020).

7. *Karpova N.E., Panfilova I.E.* Ensuring the safety of information processes in sociotechnical systems based on an analysis of the behavioral characteristics of a person as a subject of such a system // 2019 XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP). – Samara, Russia, 2019. – P. 751–753.

Корганова Ольга Георгиевна, кандидат технических наук, доцент кафедры информационно-измерительной техники Самарского государственного технического университета. Основное направление научных исследований – автоматизированные информационно-измерительные системы. Имеет более 150 публикаций. E-mail: annuin@mail.ru

Панфилова Ирина Евгеньевна, магистрант кафедры вычислительной техники Самарского государственного технического университета. Основное направление научных исследований – автоматизированные интеллектуальные системы. Имеет более 6 публикаций. E-mail: panfilova_2015@bk.ru

DOI: 10.17212/2307-6879-2020-1-2-89-98

Model of information risk management of a sociotechnical system based on human behavioral features*

O.G. Korganova[1], I.E. Panfilova[2]

[1] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, candidate of technical sciences, docent of the information measuring equipment department. E-mail: annuinr@mail.ru*
[2] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, masters student of the computer engineering department. E-mail: panfilova_2015@bk.ru*

The difficulties associated with the description and prediction of human behavior and its presence in sociotechnical systems (STS) leads to the emergence of a number of specific tasks related to ensuring the information security of STS and its integrity. The article analyzes the general and specific threats to information security that arise in the STS, considers the features of the functioning of sociotechnical systems, and also provides the logic for constructing an information risk management system implemented in the structure of the STS and taking into account behavioral characteristics of a person (goal-setting function), to ensure the safety of information processes in the STS.

Keywords: information security, behavior analysis, sociotechnical system, information processes, threat analysis

REFERENCES

1. Vasil'kov A.V., Vasil'kov A.A., Vasil'kov I.A. *Informatsionnye sistemy i bezopasnost'* [Information systems and security]. Moscow, Forum Publ., 2013. 528 p.

2. Zapechnikov S.V. *Informatsionnaya bezopasnost' otkrytykh sistem* [Information security of open systems]. In 2 vol. Moscow, GLT Publ., 2018.

3. *Kak sistemy bezopasnosti analiziruyut povedenie pol'zovatelei* [How security systems analyze user behavior]. Available at: https://clck.ru/Nctid (accessed 08.07.2020).

4. Kravchenko S.I. Bezopasnost' sotsiotekhnicheskikh sistem [The security of socio-technical systems]. *NBI Tekhnologii = NBI Technologies*, 2018, vol. 12, no. 2, pp. 20–24.

5. Ostapenko G.A., Meshkova E.A. *Informatsionnye operatsii i ataki v sotsiotekhnicheskikh sistemakh: organizatsionno-pravovye aspekty protivodeistviya* [Information operations and attacks in sociotechnical systems: organizational and legal aspects of counteraction]. Moscow, Hotline-Telecom Publ., 2007. 295 p.

* *Received 15 May 2020.*

6. Green D. *Socio-technical systems in global markets*. 2010, 23 August. Available at: http://nuleadership.wordpress.com/2010/08/23/socio-technical-systems-in-global-markets/ (accessed 08.07.2020).

7. Karpova N.E., Panfilova I.E. Ensuring the safety of information processes in sociotechnical systems based on an analysis of the behavioral characteristics of a person as a subject of such a system. *2019 XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP)*, Samara, Russia, 2019, pp. 751–753.

Для цитирования:

Корганова О.Г., Панфилова И.Е. Модель управления информационными рисками социотехнической системы на основе поведенческих особенностей человека // Сборник научных трудов НГТУ. – 2020 – № 1–2 (97). – С. 89–98. – DOI: 10.17212/2307-6879-2020-1-2-89-98.

For citation:

Korganova O.G., Panfilova I.E. Model' upravleniya informatsionnymi riskami sotsiotekhnicheskoi sistemy na osnove povedencheskikh osobennostei cheloveka [Model of information risk management of a sociotechnical system based on human behavioral features]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta = Transaction of scientific papers of the Novosibirsk state technical university*, 2020, no. 1–2 (97), pp. 89–98. DOI: 10.17212/2307-6879-2020-1-2-89-98.