КОДИРОВАНИЕ И ЗАЩИТА ИНФОРМАЦИИ

Юрьева Р.А., Комаров И.И., Дородников Н.А.

ПОСТРОЕНИЕ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ МУЛЬТИАГЕНТНОЙ РОБОТОТЕХНИЧЕСКОЙ СИСТЕМЫ С ДЕЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ

Аннотация: *Приоритетной целью нарушителя, в рассматриваемом аспекте, является препятствование выполнению поставленных задач роем роботов всеми возможными способами, вплоть до их уничтожения. Главной задачей системы информационной безопасности является предоставление должного уровня безопасности роя роботов, от всех возможных естественных и искусственных препятствий. аспекте данной работы, необходимо учитывать не только информационную защиты активов, но и их физическую защищенность. Для широкого круга объектов (назовем их объектами потенциального воздействия нарушителей - ОПВН) для обеспечения их физической защиты очень важна разработка перечня потенциальных угроз и, прежде всего, проектной угрозы. Только она позволяет адекватно спроектировать необходимую систему физической защиты конкретного объекта, а затем и предметно оценить ее эффективность. Составным элементом проектной угрозы является модель нарушителя, поэтому формирование данной модели - актуальная задача. Согласно руководящим документам, модель нарушителя должна формироваться, исходя, как из особенностей объекта и технологических операций, выполняемых на нем (стабильные факторы), так и изменяющихся факторов - социальных условий, складывающихся в районе расположения объекта и в самом коллективе предприятия, социально-психологических особенностей отдельных групп людей и личностей, а также обстановки в мире, стране, регионе и т.п. Таким образом, в одной модели должны учитываться многообразные факторы, относящиеся к разным аспектам действительности, зачастую не связанные между собой. В данной статье предложенные модели рассматривают нарушителя с разных точек зрения. Тем не менее, данные модели связаны между собой, изучение этих связей - одна из задач анализа уязвимости. Если полученные*

DOI: 10.7256/2305-6061.2016.1.17946

характеристики ОМН ниже ПМН (например, численность агентов-нарушителей, которые, по оценке ситуации, могут быть сегодня задействованы в деструктивном воздействии, меньше численности нарушителей данного вида, на пресечение действий которых спроектирована СЗИ в соответствии с предписанной объекту проектной угрозой, Z>У), то возможно принятие решения о достаточной защищенности объекта, то есть о том, что в данный момент нет необходимости в проведении каких-либо внеплановых действий (анализа уязвимости объекта с оценкой эффективности его СЗИ, совершенствования СЗИ, изменения технологии выполения задачи и пр.).

Ключевые слова: *информационная безопасность, мультиагентная робототехническая система, децентрализованное управление, модель нарушителя, моделирование, роботизированная система, деструктивное воздействие, роевая робототехника, дезорганизованное поведение, защитные меры*

Abstract: *The primary objective of the interloper is to keep a swarm of robots from performing their functions by any means including their destruction. The primary goal of the information security system is to provide the proper security level for the swarm of robots against any natural or artificial hindrances for it is necessary to take into account not only the information safety but also physical security of actors. For the physical security of a wide range of facilities (the authors offer to call them 'facilities under potential interloper's influence or FPIP) it is very important to prepare the list of potential threats, especially design threats. The list would allow to design a necessary system for the physical protection of a particular facility and to evaluate its efficiency. The composite element of the design threat is the interloper modeling and therefore development of such a model is a high priority. According to the guideline documents, the interloper model should be based on both the features of the facility and performed technological operations (stable factors) and variable factors, i.e. social conditions of the territory where the facility is located, social relations, psychological traits of a particular group of workers and/or individuals as well as the global, country's, regional environment, etc. Therefore, the model should take into account all kinds of factors that are related to various aspects of the reality and often divorced from one another. The authors of the present article analyze the offered interloper models from different points of view. Nevertheless, these models are interconnected, so examination of these connections is one of the goals of the vulnerability analysis. In case the obtained characteristics of the operational interloper model are below the desired characteristics of the design interloper model (for example, the number of interloper agents that can be potentially involved in the destructive activity is lower than the number of interlopers which activities are to be prevented by the designed Information Security System according to the design project prescribed for the facility, i.e. Z>У), then the decision about sufficient facility hardness can be made meaning there is no need to perform unscheduled actions (facility vulnerability analysis with ISS performance evaluation, improvement of ISS, changes in the task execution technology, etc.).*

Keywords:*information security, multi-agent robotic system, decentralized control, interloper model, modeling, robotic system, destructive influence, swarm robotechnics, disorganized behavior, protective measures*

DOI: 10.7256/2305-6061.2016.1.17946

Построение модели вероятностного нарушителя безопасности информации и модели угроз, актуальной для конкретной информационной системы (ИС), - основа для построения эффективной системы безопасности.

Согласно руководящим документам, модель нарушителя должна формироваться, исходя, как из особенностей объекта и технологических операций, выполняемых на нем (стабильные факторы), так и изменяющихся факторов - социальных условий, складывающихся в районе расположения объекта и в самом коллективе предприятия, социально-психологических особенностей отдельных групп людей и личностей, а также обстановки в мире, стране, регионе и т.п. Таким образом, в одной модели должны учитываться многообразные факторы, относящиеся к разным аспектам действительности, зачастую не связанные между собой. Это свидетельствует о том, что в модели с точки зрения системного подхода отсутствует учет принципа множественности описания сложных систем, а это приводит к сложностям в использовании моделей в работе. При таком подходе модель нарушителя становится самоцелью, а не средством решения конкретной практической задачи.

Нарушитель, сам по себе, тоже является системой, зачастую обладающий большей сложностью и менее изученной, следовательно, создание какой либо общей модели, учитывающей все стабильные и изменяющиеся факторы, не является целесообразным решением. Для решения этой задачи, специалисты по категорированию, анализу и оценке уязвимостей предлагают использовать одновременно три типа моделей нарушителя, условно называемых как технологическая, оперативная и проектная модели.

В рамках данного исследования предполагается разработать модель нарушителя и модель угроз для МРТС, удовлетворяющей следующим параметрам:

МРТС являются гомогенными;

- отсутствует возможность централизованного управления агентами МРТС;
- отсутствует возможность обнаружения деструктивного воздействия агентами МРТС;
- отсутствует информация об отдельных агентах МРТС;
- алгоритм предполагает изменение некоторых косвенных параметров группы, которое можно оценить до начала выполнения алгоритма;
- существует корреляция между изменением этих параметров и эффективностью работы МРТС.

Процесс разработки модели угроз безопасности МРТС состоит из следующих этапов [1-3]:

1. составление полного перечня угроз безопасности МРТС;
2. определение частоты (вероятности) реализации угроз;
3. определение коэффициентов реализуемости угроз;
4. определение показателей опасности угроз [4].

Если характеристики ОМН выше характеристик ПМН, но ниже характеристик ТМН, вероятно, могут быть приняты необходимые дополнительные меры. Скорее всего, эти меры будут касаться в большей степени не объекта, а других субъектов обеспечения безопасности ОПВН. Ввод в действие такого рода мер возможен на некоторый промежуток

DOI: 10.7256/2305-6061.2016.1.17946

времени, когда есть основания предполагать, что вызвавшие их причины не носят долговременного характера. Если же это не так или характеристики ОМН выше характеристик и ПМН и ТМН (Z<У, и У>X), то должно приниматься решение:

о совершенствовании СЗИ;

об изменении:

– технологического процесса для ликвидации его наиболее уязвимых мест;
– инфраструктуры, окружающей объект (если это возможно);
– организации функционирования внешних сил безопасности и т.п.

Предпочтительность выбора и последовательности ввода в действие мер определяется с учетом возможности реализации решения, по наличию временных, людских и финансовых ресурсов. Таким образом, фактически речь может идти о пересмотре проектной угрозы (ПМН). Вероятно, это может быть связано с причинами, которые носят долговременный характер. Важное место в этом случае должно быть отведено мерам, реализуемым другими субъектами обеспечения безопасности объекта.

Принимая во внимание все изложенное выше, можно сформировать актуальные требования к средствам защиты, при которых возможно эффективное противостояние нарушителю

Получение аналитических зависимостей, позволяющих идентифицировать аномальную активность или проявление информационных событий, вызванных диверсантами, не всегда возможно [4, 5], что позволяет выделить ряд потенциальных атак, которые направлены на нарушение целостности, конфиденциальности и доступности информации:

- активный сбор информации;
- попытки организации несанкционированного доступа;
- «отказ» в обслуживании;
- быстрый выход робота из строя (разрядка аккумулятора);
- повышенная активность.

Как правило, в опасных или труднодоступных для человека местах и используются мобильные роботы. Но если говорить об использовании роботов в условиях излишне агрессивной среды, стоит позаботиться о создании повышенного уровня прочности.

Условием, которое обязательно дабы обеспечить информационную безопасность служит сохранение единства функционирования оборудований МРТС и его устройств с остальными внешними составляющими.

Такие угрозы характеризуются нарушением режимов функционирования, или их вывод из работы. Как результат, может быть осуществлены: повышение вероятностей НСД, отказ в сервисе, искажение и потеря используемых ранее данных.

К числу форс-мажорных обстоятельств относят: пожар, излучение радиации, стихийное бедствие.

В случае отказа оборудования:

- сбой работы или отказ средств аппаратных и программных систем;
- сбой или отказы средств хранящего информацию.

DOI: 10.7256/2305-6061.2016.1.17946

В состав программных обеспечений входят:

- операционные системы;
- программное средство безопасности от НСД;
- специальные программные обеспечения, направленные на обработку и сохранение информаций, находящихся в ограниченном доступе.

К числу человеческих факторов относят:

- ошибка или ряд ошибок программного обеспечения;
- произведение непреднамеренных действий пользователем, во время работы программного обеспечения;
- внедрение и разработку вирусных кодов в закладку программного обеспечения;
- осуществление преднамеренных действий пользователем, во время использования программного обеспечения.

К умышленным действиям относят: действия, которые были совершены пользователем преднамеренно, для получения НСД.

К неумышленным действиям относят: действия, которые были произведены по ошибке, и в результате чего, выполняется НСД.

Личность человека, совершающего преступление, по причине характерных для него психологических особенностей, антиобщественных взглядов, негативного отношения к этическим нормам и предпочтение в выборе противозаконных методов, в угоду своим нуждам или бездействие в предотвращении отрицательного результата, определяется как нарушитель.

Специфическая сущность личности нарушителя заключается в особенностях его психического склада, которые выражают собой внутренние предпосылки антиобщественного поведения. Общественная опасность выражает потенцию личности к преступному поведению, которая понимается как внутренняя возможность совершения при определенных условиях преступных действий.

Выделяют два вида нарушителей по чертам, присущим его характеру поведения

1) Осторожные нарушители характеризуются:
1.1) низким уровнем тревожности
1.2) общительностью, стремятся установить контакт с сотрудниками
1.3) низким порогом ответственности за содеянные преступления
2) Неосторожные нарушители характеризуются:
2.1) высоким уровнем тревожности
2.2) проявлением неуверенности в себе
2.3) дезорганизованность поведения
2.4) в экстремальных ситуациях реализуют эмоциональные, а не рациональные реакции.

Для осуществления своих планов нарушитель может использовать всевозможные методы получения информации, ограниченные только его технической оснащенностью и знаниями.

Выделены следующие наиболее актуальные способы получения информации о деятельности роя на местности:

DOI: 10.7256/2305-6061.2016.1.17946

1. Наблюдение. Данный вид деятельности нарушителя является наименее агрессивным и продуктивным. Он способен дать лишь поверхностную информацию о целях, количестве и местоположении членов роя.
2. Захват робота. Данный способ предоставляет нарушителю возможность получения секретной информации непосредственно из робота и/или, перепрограммировав его дальнейший мониторинг деятельности роя.
3. Перехват передаваемой информации. Данный способ предоставляет нарушителю секретную информацию, передаваемую по каналам связи, для осуществления необходимо иметь специальное прослушивающее оборудование.
4. Использование одного или группы роботов-диверсантов. Использование роботов-диверсантов является наиболее опасной угрозой, так как возможно воздействие, как на физическом уровне, так и на уровне передачи информации.

Позиция оправданного пессимизма позволяет предположить, что нарушитель способен на использование как минимум двух способов получения информации, наиболее же актуальной и привлекательной, с точки зрения нарушителя является возможность захвата робота.

Из предоставленного материала можно сделать следующие выводы:

— технология РРТС находится в развитии, следовательно, модели нарушителя и угроз будут развиваться параллельно ей, поэтому целесообразно ожидать появления новых технологий и факторов развития.

— описание модели нарушителя осуществляется на основе применения методов теории управления рисками и технико-экономического анализа.

Ознакомившись со все возможными угрозами, которые могут воздействовать на эффективную работу и сохранность робота, можно заявить, что МРТС является слабо защищенным, уязвимым объектом. Наибольший ущерб для МРТС приносят атаки на неё изнутри, например, когда взломщик (робот-шипон) зарегистрировался в системе и способен выполнять команды от её имени. Физический вред на технологические компоненты робота можно нанести чем угодно т. к. робот не оснащен каким-либо крепким «щитом», который может обезопасить себя от физических воздействий. Так же плохо защищены каналы коммуникаций робота, что может привести к НСД к технологическим компонентам робота.

Библиография :

1. Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // «Научно-технический вестник информационных технологий, механики и оптики». № 5(87), НИУ ИТМО, СПб., 2013. С. 149-154.
2. Зикратов И.А., Одегов С.В., Смирных А.В. Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования // Научно-технический вестник информационных технологий, механики и оптики -2013. № 1(83). С. 141-144.

DOI: 10.7256/2305-6061.2016.1.17946

3. Арустамов С.А., Дородников Н.А., Дородникова И.М Проблемы эксплуатации корпоративных сетей, выявление их причин // «Научные труды sworld». 2013. № 4, "Научный мир", Иваново. Т. 12. С. 62-66.
4. Арустамов С.А., Генин М.Г. Деревья ущербов как модель оценки рисков потерь доступности после проведения изменений в финансовых информационных системах // «Научно-технический вестник информационных технологий, механики и оптики». № 2(84), НИУ ИТМО. СПб., 2013. С. 129-135.
5. Карпов В.Э. Управление в статических роях. Постановка задачи // «Интегрированные модели и мягкие вычисления в искусственном интеллекте» Сб. научных трудов VII –й Международной научно-практической конференции (Коломна, 20–22 мая 2013). С. 12.
6. Iñaki Navarro and Fernando Matía An Introduction to Swarm Robotics.ETSI Industriales, Universidad Politécnica de Madrid, c/José Gutiérrez Abascal, 2, 28006 Madrid, SpainReceived 18 April 2012; Accepted 19 June 20127 F. Higgins, A. Tomlinson, and K.M. Martin, "Survey on security challenges for swarm robotics," in Proceedings of the 5th International Conference on Autonomic and Autonomous Systems (ICAS '09), p. 307–312, IEEE Computer Society, Los Alamitos, CA, USA, April 2009.

References:

1. Zikratov I.A., Kozlova E.V., Zikratova T.V. Analiz uyazvimostei robototekhnicheskikh kompleksov s roevym intellektom // «Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki». № 5(87), NIU ITMO, SPb., 2013. S. 149-154.
2. Zikratov I.A., Odegov S.V., Smirnykh A.V. Otsenka riskov informatsionnoi bezopasnosti v oblachnykh servisakh na osnove lineinogo programmirovaniya // Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki -2013. № 1(83). S. 141-144.
3. Arustamov S.A., Dorodnikov N.A., Dorodnikova I.M Problemy ekspluatatsii korporativnykh setei, vyyavlenie ikh prichin // «Nauchnye trudy sworld». 2013. № 4, "Nauchnyi mir", Ivanovo. T. 12. S. 62-66.
4. Arustamov S.A., Genin M.G. Derev'ya ushcherbov kak model' otsenki riskov poter' dostupnosti posle provedeniya izmenenii v finansovykh informatsionnykh sistemakh // «Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki». № 2(84), NIU ITMO. SPb., 2013. S. 129-135.
5. Karpov V.E. Upravlenie v staticheskikh royakh. Postanovka zadachi // «Integrirovannye modeli i myagkie vychisleniya v iskusstvennom intellekte» Sb. nauchnykh trudov VII –i Mezhdunarodnoi nauchno-prakticheskoi konferentsii (Kolomna, 20–22 maya 2013). S. 12.
6. Iñaki Navarro and Fernando Matía An Introduction to Swarm Robotics.ETSI Industriales, Universidad Politécnica de Madrid, c/José Gutiérrez Abascal, 2, 28006 Madrid, SpainReceived 18 April 2012; Accepted 19 June 20127 F. Higgins, A. Tomlinson, and K.M. Martin, "Survey on security challenges for swarm robotics," in Proceedings of the 5th International Conference on Autonomic and Autonomous Systems (ICAS '09), p. 307–312, IEEE Computer Society, Los Alamitos, CA, USA, April 2009.

DOI: 10.7256/2305-6061.2016.1.17946