УДК 004.056

Е. В. БРЕЖНЕВ, Е. В. БРОШЕВАН, А. С. КАРПЕНКО

Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Харьков, Украина

МЕТОД ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИУС С ИСПОЛЬЗОВАНИЕМ БАЙЕСОВСКОЙ СЕТИ ДОВЕРИЯ

Предлагается метод анализа рисков информационной безопасности (ИБ) ИУС, который учитывает взаимовлияние между состояниями ИБ ее активов. Метод основан на построении графовероятностной модели рисков ИБ, в основе которой лежит использование байесовской сети доверия (БСД). Приводится иллюстративный пример использования метода для SCADA системы. Разработанный метод позволяет оценить уровень ИБ ИУС, прогнозировать изменение уровней ИБ ее взаимосвязанных активов, формировать сценарии возможных атак и их последствия, а также формировать множество контрмер по снижению этих рисков. Использование метода позволяет рационально использовать существующие ресурсы ИУС для контроля рисков активов и решать задачи их перераспределения с учетом взаимовлияния между состояниями ИБ.

Ключевые слова: *БСД, ИУС, оценка рисков, инциденты, информационная безопасность.*

Введение

Современный уровень развития информационных технологий (ИТ) позволяет использовать возможности вычислительных средств для минимизации негативного влияния человеческого фактора на управление технологическими процессами (ТП) и повышения их экономической эффективности. Так, например, внедрение информационно-управляющих систем (ИУС), обеспечивающих автоматизированный сбор и обработку информации для управления сложным технологическим объектом, позволяет оптимизировать ТП за счет возможности удаленного доступа к объекту с целью обслуживания, сбора информации о технологических параметрах, обнаружения и предотвращения аварийных ситуаций и т.п.

Интенсивное развитие ИУС особенно остро ставит вопрос их защиты как от угроз техногенного и антропогенного характера, так и от угроз информационной безопасности [1]. Защита ИУС важна, поскольку ущерб, связанный с отказами и сбоями в их работе, приводит не только к финансовым потерям, но и к рискам потери человеческих жизней, здоровья, возникновения экологических катастроф.

1. Проблема ИБ для ИУС

Вопросам информационной безопасности (ИБ) ИУС до недавнего времени не уделялось должного внимания, что и стало одной из причин ряда инцидентов, связанных с нарушением ИБ.

В общем случае ИБ объекта предполагает сохранение конфиденциальности, целостности и доступности информации [2]. Основной целью обеспечения ИБ ИУС является поддержание ее необходимого уровня, снижение рисков и угроз, связанных с несанкционированным доступом, нарушением целостности информации, обеспечение нормального функционирования объекта эксплуатации [3].

Классифицируя информационные атаки на ИУС по способу реализации и последствиям, можно выделить следующие основные типы: DoS атаки на WEB-сервисы ИУС, внедрение в ПО вредоносного программного кода – угрозы целостности и доступности и несанкционированный доступ (НСД) к сервисам и ресурсам ИУС – угроза как целостности и доступности информации, так и ее конфиденциальности [4].

Можно привести множество примеров инцидентов, связанных с угрозами ИБ ИУС. Так, например:

1. В 2003 г. произошло заражение вирусом Slammer ИУС энергетической станции Davis-Besse, вызвавшее сбои в её работе (США, Огайо). Вирус заразил большое количество рабочих станций, попав в оборудование через незащищенный канал связи. Это привело к потере контроля над состоянием реакторов [5]. Это типичная угроза доступности системы, что является наиболее критичным для таких систем, как ИУС, которая относится к системам реального времени.

2. В 2006 г. произошел инцидент на АЭС Browns Ferry (США, Алабама), где в результате по-

лучения аномального сетевого трафика из производственной сети были выведены из строя программируемые логические контроллеры (ПЛК), что вызвало аварийное выключение реактора станции [6]. Данный инцидент является типичным примером DoS атаки, которая приводит к потере доступности и целостности системы.

3. В 2010 г. произошло заражение системы Supervisory Control and Data Acquisition (SCADA) промышленным вирусом Stuxnet [7]. Вирус мог использоваться в качестве средства несанкционированного сбора данных и диверсий в системе. Вирус проникал в систему через ПК сотрудников, заражал ПО автоматизации, перехватывал управление ПЛК и был способен его перепрограммировать и как следствие – проводить манипуляции данных SCADA. Этот инцидент является примером реализации угроз ключевым параметрам ИБ: конфиденциальности, целостности, доступности.

Следует отметить, что защищенность компонентов ИУС от угроз ИБ может характеризоваться уровнем ИБ компонентов, подсистем и ИУС в целом. Уровень ИБ может быть определен уровнем рисков и угроз, которые могут привести к нарушениям ИБ системы, компонентов ИУС.

Анализ приведенных выше инцидентов подтверждает существование причинно-следственных связей между уровнями ИБ активов ИУС (ее систем, компонентов, пр.) Так, снижение уровня ИБ одного из активов может привести к снижению уровней ИБ актива, связанного с ним. Таким образом, можно говорить о “перетекании” рисков ИБ между активами. Риски ИБ “передаются” от актива к активу за счет существующих связей (информационных, логических, пр.) между ними.

ИБ ИУС не является интегральной составляющей уровней ИБ ее активов. Взаимовлияние и связь между активами приводит к появлению новых эмерджентных рисков ИБ, не свойственных данным активам.

В настоящее время существует множество подходов, описывающих меры защиты и политику безопасности промышленных систем управления и контроля. Так, например, стандарт NIST SP 800-82 Guide to Industrial Control Systems Security [8] дает рекомендации по обеспечению безопасности SCADA систем, описывает их топологии, определяет типовые угрозы и уязвимости, предоставляет рекомендации по контрмерам для угроз ИБ.

В нормативном документе NISTIR 7628 Guidelines for Smart Grid Cyber Security[9] описывается кибербезопасность в Smart Grid (адаптивно-активных электросетях), устанавливаются профили безопасности, и описывается взаимосвязь подсистем и их угроз с точки зрения необходимости обеспечения целостности, конфиденциальности и доступности [10].

Кроме того, существует множество различных научных подходов к оцениванию ИБ ИУС. Так, например, особенностью подхода, предложенного в работе [11], является использование ориентированного графа компрометации системы, узлы которого – этапы потенциальных атак, а ребра соответствуют ожидаемому времени осуществления атаки в зависимости от уровня навыков атакующего.

В работе [12] риск анализ используется для определения самой уязвимой подстанции и наиболее критического актива в этой подстанции с целью своевременной разработки комплекса мер по контролю уязвимостей и предотвращения кибератак.

Недостатком упомянутых подходов является то, что они не учитывают взаимосвязи между рисками активов и не учитывают связи между состояниями ИБ этих активов. ИУС обладают сложной природой взаимовлияния. Объединение активов в рамках ИУС приводит к появлению эмерджентных рисков, не связанных непосредственно с самими активами. Это обусловлено взаимным влиянием между уровнями ИБ различных активов.

Таким образом, с одной стороны ИТ приводят к оптимизации управления ТП и объектами, а с другой, вносят новые уязвимости в эти системы, что приводит к появлению новых рисков, уже не связанных непосредственно с самой системой и технологиями ее реализации, архитектурой, сетевыми решениями, пр. Внедрение ИТ приводит к усилению взаимовлияния между уровнями ИБ активов ИУС. В этой связи возникает задача оценки рисков ИБ ИУС с учетом взаимовлияния между уровнями ИБ ее систем, компонентов (активов) и разработки подхода к учету влияния между уровнями ИБ активов ИУС.

Цель статьи – разработка метода оценивания рисков ИБ ИУС с учетом взаимовлияния между уровнями ИБ ее активов.

2. Разработка метода оценки рисков ИБ ИУС

Под риском ИБ, в соответствии с ISO/IEC 27000:2009 [2], понимается потенциальная возможность того, что угроза будет использовать уязвимость актива или группы активов, причиняя, таким образом, ущерб объекту.

Анализ рисков ИБ состоит в том, чтобы оценить величину этих рисков, в терминах вероятности инцидента и тяжести его последствий, определить меры по их уменьшению и затем убедиться, что риски снижены до приемлемого уровня. Основу процесса составляет определение того, что надо защищать, от кого и как. Для этого выявляются акти-

вы ИУС и для каждого из них строится матрица риска, которая показывает взаимосвязь между вероятностью реализации угрозы и величиной ущерба при ее реализации.

Состояние ИБ может рассматриваться как состояние отсутствия рисков для основных атрибутов ИБ актива – целостности, конфиденциальности, доступности. Состояние ИБ характеризуется уровнем защищенности ИБ активов ИУС от различного рода угроз.

В рамках данного метода предлагается использовать элементы методологии, предложенной в стандарте NIST SP800-30 [13] (рис.1).

Метод, предлагаемый в рамках данной работы, включает следующие этапы:

1. Анализ аппаратных средств, ПО, системных интерфейсов, данных и информации, подготовки персонала с целью определения множества активов ИУС, важных для ИБ.
2. Анализ нарушений ИБ, которые имели место в системе, и их последствий.
3. Анализ отчетов проведенных аудитов безопасности, технических мероприятий, связанных с поиском уязвимостей.
4. Оценка текущих и планируемых мер защиты для определения вероятности угрозы через уязвимость.
5. Вероятностный анализ использования уязвимостей.
6. Оценка величины ущерба при реализации угрозы.
7. Оценка уровня рисков в системе. Определение риска для пары угрозы/уязвимости может быть выражено как функция от: вероятности того, что данный источник угрозы использует данную уязвимость; величины воздействия; достаточности мер защиты. Определение уровней рисков производится с помощью матриц рисков на основе обработки полученных раннее оценок. В качестве результатов – оценки уровней рисков ИБ: «Высокий», «Средний» и «Низкий».
8. Определение множества связей активов ИУС, которые приводят к распространению (передаче) рисков ИБ между ними.
9. Построение БСД с учетом взаимовлияния между состояниями ИБ активов.
10. Анализ полученных данных. Результатом этого этапа является подробное описание БСД с учетом взаимовлияния рисков активов.
11. Определение мер защиты, которые могут снизить или устранить идентифицированные риски ИУС.
12. Формирование документа, описывающего результат проделанной работы – отчет о проведенном аудите и анализе ИБ системы.

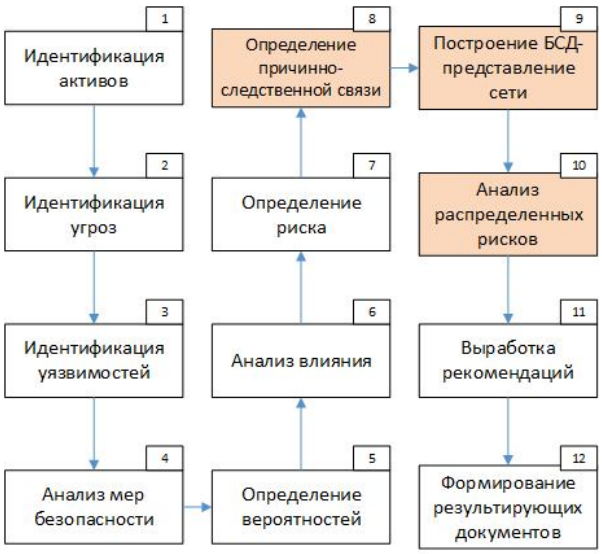

Рис. 1. Действия анализа рисков

Этапы 8-10 демонстрируют суть предлагаемого метода анализа рисков.

Задача оценки взаимного влияния состояний ИБ активов может быть решена за счет построения БСД (графическая вероятностная модель ИБ).

В БСД вероятности пребывания актива S_3 в различных состояниях ИБ из множества Ω_{S3} в зависимости от состояний ИБ других активов ИУС могут быть определены по соотношению вида:

$$P(S_3^{(k)}) = \sum_i \sum_j P(S_3^{(k)} / S_1^{(i)}, S_2^{(j)}) * P(S_1^{(i)}) * P(S_2^{(j)}), \quad (1)$$

где $P(S_3^{(k)})$ - вероятность нахождения актива S_3 в k-м состоянии ИБ;

$P(S_3^{(k)} / S_1^{(i)}, S_2^{(j)})$ - условная вероятность нахождения актива S_3 в k-м состоянии ИБ при условии нахождения актива S_1 в i – м состоянии ИБ и актива S_2 в j – м состоянии ИБ;

$P(S_1^{(i)})$ - вероятность нахождения актива S_1 в i-м состоянии ИБ;

$P(S_2^{(j)})$ - вероятность нахождения актива S_2 в j-м состоянии ИБ.

Узлами БСД являются активы ИУС. Переменной, описывающей каждый актив, является состояние ИБ, описываемое уровнем ИБ - лингвистической переменной (ЛП) «Высокий», «Средний», «Низкий».

Между состояниями ИБ в БСД существуют связи, определяющие зависимости между уровнями рисков, представленные в виде таблицы условных вероятностей.

3. Иллюстрация метода на примере SCADA системы

В рамках данной работы будет рассматриваться архитектура ИУС, представленная на Рисунке 2.

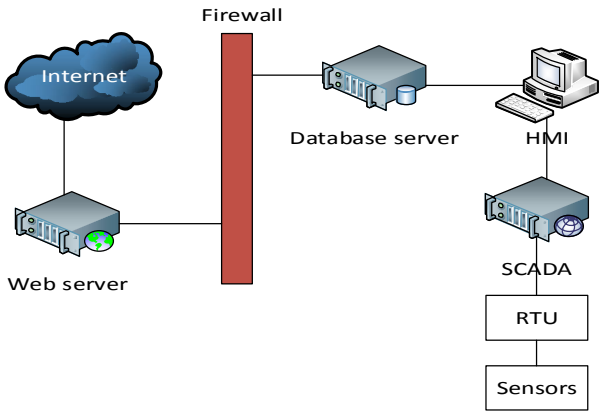

Рис. 2. Пример архитектура SCADA (удаленная атака на веб-сервер)

Ввиду большого количества возможных угроз, для иллюстрации предложенного метода будет рассмотрен такой вектор атаки (направление воздействия на объект защиты со стороны потенциального злоумышленника), как веб-вектор, использующий веб-ресурс, на примере SQL-injection.

SQL-injection – вредоносный код, который способен заразить рабочие станции и сервера. Возможная угроза доступности – заражение и сбой в работе рабочих станций и серверов, используемых для обработки информации. Далее, поэтапно описывается предлагаемый метод на примере.

1. Идентификация активов

Как представлено на Рисунке 2, система состоит из трех уровней. На нижнем уровне расположены сенсоры и элементы контроля. В уровне ячейки расположен RTU (Real Time Unit). И наконец, на стационарном уровне располагаются Web-сервер, сервер базы данных и сервер SCADA системы.

2. Идентификация угроз

Применение веб-технологий в SCADA системах приводит к дополнительным угрозам. В рамках примера рассматривается угроза SQL-инъекций, которая ведет к различным манипуляциям с базой данных, рискам утечки информации и даже к отказу системы.

3. Идентификация уязвимостей

SCADA-система находится в стадии проектирования, в связи с этим сведенья о нарушениях безопасности отсутствуют.

4. Анализ мер безопасности

Ввиду того, что система имеет трехуровневую структуру, то предполагается, что каждый уровень отделен от другого межсетевым экраном.

5. Определение вероятностей

Вероятностные значения определяются экспертной оценкой на основании типичных угроз/уязвимостей таких систем.

6. Анализ влияния

Величина ущерба от SQL-инъекций - это, прежде всего, утечка конфиденциальной информации, а также выполнение системных команд, которые за собой ведут возможные экономические потери, риски окружающей среде. В рамках примера, потери могут составлять утечку информации, которая имеет коммерческую ценность, а также потерю управления над всей системой.

7. Определение риска

Величина риска состоит из двух параметров: вероятность происшествия и тяжесть возможных последствий (Рисунок 3). Для расчета используется формула: РИСК = Р(происшествия) * Ущерб (ПОТЕРИ). Расчет риска также основывается на экспертной оценке.

8. Определение причинно-следственных связей

Исходя из представленной архитектуры системы (Рисунок 2), повышение уровня риска Web-сервера влечет за собой повышение уровня риска для сервера базы данных, дальше риск “распространяется” по стационарной шине, увеличивая локальные риски, воздействуя на человеко-машинный интерфейс и на SCADA-сервер. В свою очередь состояние ИБ SCADA-сервера влияет на состояние ИБ RTU. Эти связи приводят к распространению рисков по системе.

9. Построение БСД сети

При помощи графического редактора NETICA (версии 5.18 от 2014 года), была построена графическо-вероятностная модель ИБ, узлами которой являются активы системы с указанными состояниями ИБ (Рисунок 3). Уровни ИБ могут быть получены с использованием экспертных методов.

10. Анализ распределенных рисков

С учетом представленной на Рисунке 3 графическо-вероятностной модели ИБ системы, можно предположить, что при реализации атаки типа SQL – инъекция, которая нацелена на базу данных, происходит изменение уровня ИБ последнего (Рисунок 4). Следовательно, с увеличением риска для базы данных, появляются дополнительные риски ИБ для всех активов, увеличивая их для человеко-машинного интерфейса, SCADA-сервера, стационарной шины и т.д.

11. Выработка рекомендаций

Для защиты SCADA от атак типа SQL – инъекция необходимо:

– обеспечить фильтрацию запросов к базе данных;

– составить «белый» список;

– добавить к каждой связке активов межсетевые экраны.

12. Формирование результирующих документов

Результат применения метода документируется в виде отчета об аудите ИБ, которая включает в себя информацию о проведенном анализе системы, выявленных рисках, взаимовлияниях между активами и рекомендации по их снижению.

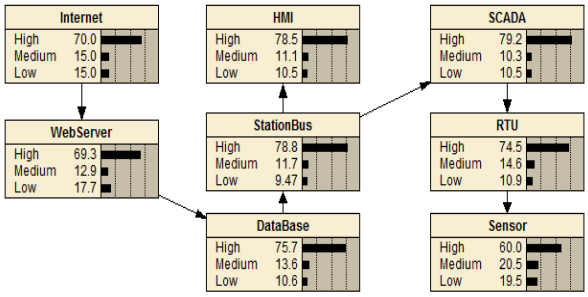

Рис. 3. Система активов SCADA до реализации угрозы

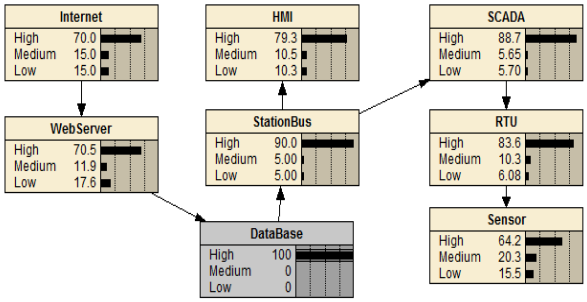

Рис. 4. Система активов SCADA после реализации угрозы

Заключение

Разработанный метод позволяет оценить уровень ИБ ИУС, прогнозировать изменение уровней ИБ взаимосвязанных активов, формировать сценарии возможных атак и их последствия. Использование метода позволяет рационально использовать существующие ресурсы ИУС для контроля рисков активов и решать задачи их перераспределения с учетом взаимовлияния между состояниями ИБ.

В рамках данного подхода это взаимовлияние предлагается оценивать с использованием БСД. Преимуществом применения БСД является возможность прогнозирования изменений уровней рисков взаимосвязанных активов. Это позволяет комплексно оценить уровень ИБ системы и предпринять соответствующие меры.

БСД позволяет прогнозировать изменение уровней рисков актива ИУС при изменении рисков активов, связанных с ним. Это позволяет проводить риск-мониторинг информационной безопасности в ИУС.

Кроме того, данный метод позволяет прогнозировать возможные сценарии вектора атак и перераспределять средства снижения рисков и выбора контрмер с учетом их стоимости.

Литература

1. Надеждин, Ю. В. Безопасность АСУ ТП критически важных объектов [Электронный ресурс] / Ю.В. Надеждин. – Режим доступа: http://www.uipdp.com/articles/2014-04/06.html. – 17.03.2014.

2. Ницель, Л. В. 6 шагов к информационной безопасности АСУ ТП [Электронный ресурс] / Л. В. Ницель – Режим доступа: http://ua.automation.com/content/6-shagov-k-informacionnoj-bezopasnosti-asu-tp. – 15.07.2014.

3. Гарбук, Н. В Стандартизация в области обеспечения информационной безопасности АСУ ТП [Электронный ресурс] / Н. В. Гарбук. – Режим доступа: http://www.slideshare.net/phdays/ss-836 0192. – 25.08.2014.

4. Лукацкий, А. В. Безопасность АСУ ТП: от слов к делу [Электронный ресурс] / А. В. Лукацкий Режим доступа: http://www.slideshare.net/lukatsky/ss-14279925. – 30.08.2014

5. Воронцов, А. Л. Автоматизированные системы управления технологическими процессами. Вопросы безопасности [Электронный ресурс] / А. Л Воронцов. – Режим доступа: http://www.jetinfo.ru/stati/informatsionnaya-bezopasnost-promyshlennykh-obektov/2011/?nid=77f3dbdaa8 dfb77077c0888a712a3e1a. – 2.09.2014.

6. Юдин, А. А. Анализ и оценка нормативных документов, применяемых для обеспечения информационной безопасности SMART GRID систем [Электронный ресурс] / А. А. Юдин, Г. В. Пирогов. – Режим доступа: http://pnzzi.kpi.ua/25/25_p88.pdf. –05.10.2014

7. Stoneburner, Gary. NIST SP 800-30, Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Electronic resource] / Gary Stoneburner, Alice Goguen, Alexis Feringa. – National Institute of Standards and Technology, July 2002. – 54 p. – Access mode: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. – 12.10.2015.

8. Варфоломеев, А. А. Управление информационными рисками [Текст] : учеб. пособие / А. А. Варфоломеев. – М. : РУДН, 2008. – 158 с.

9. Frigault, M. Measuring network security using bayesian network-based attack graphs [Electronic resource] / M. Frigault and L. Wang // In Computer Soft-

ware and Applications, 2008. COMPSAC '08. 32nd Annual IEEE International. – DOI:10.1109/COMPSAC.2008.88. – Access mode: http://www.researchgate.net/publication/4363644_Measuring_Network_Security_Using_Bayesian_Network-Based_Attack_Graphs. – 12.05.2015.

10. Frigault, M. Measuring network security using dynamic bayesian network [Electronic resource] / M. Frigault, L. Wang, A. Singhal, S. Jajodia // In Proceedings of the 4th ACM workshop on Quality of protection, 2008. – P. 23-30. http://dl.acm.org/citation.cfm?id=1456368. –12.05.2015.

11. Finn, V. Jensen. Bayesian Networks and Decision Graphs [Text] /V. Jensen Finn. – New York : Springer-Verlag, 2001. – 280 p.

12. Burroughs, D. Analysis of Distributed Intrusion Detection Systems Using Bayesian Methods [Text] / D. Burroughs, L. Wilson, G. Cybenko // Performance, Computing, and Communications Conference, 2002. 21st IEEE International, 2002. – P. 329 –334.

13. Heckerman, D. Bayesian Networks for Data Mining [Text] / D. Heckerman // Data Mining and Knowledge Discovery. – 1997. – № 1. – P. 79–119.

14. Cheeseman, P. Bayesian classification (AutoClass): theory and results [Text] / P. Cheeseman, J. Stutz // In Advances in Knowledge Discovery and Data Mining ; edited by U. M. Fayyad et al. – California : The AAAI Press, 1996. – P. 153-180.

Поступила в редакцию 2.11.2015, рассмотрена на редколлегии 18.11.2015

МЕТОД ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІУС З ВИКОРИСТАННЯМ БАЙЄСОВСЬКОЇ МЕРЕЖІ ДОВІРИ

Є. В. Брежнєв, Є. В. Брошеван, А. С. Карпенко

Пропонується метод аналізу ризиків інформаційної безпеки (ІБ) ІУС, який враховує взаємовплив між станами ІБ та її активів. Метод засновано на побудові графо-ймовірнісної моделі ризиків ІБ, в основі якої лежить використання байєсовської мережі довіри (БМД). Розглядається ілюстративний приклад використання методу для SCADA системи. Розроблений метод дозволяє оцінити рівень ІБ ІУС, прогнозувати зміну рівнів ІБ її взаємопов'язаних активів, формувати сценарії можливих атак та їх наслідки, а також формувати безліч контрзаходів щодо зниження цих ризиків. Використання методу дозволяє раціонально використовувати існуючі ресурси ІУС для контролю ризиків активів і вирішувати завдання їх розподілу з урахуванням взаємовпливу між станами ІБ.

Ключові слова: БМД, ІУС, оцінка ризиків, інциденти, інформаційна безпека.

METHOD OF RISK EVALUATION OF INFORMATION SECURITY OF ICS USING BAYESIAN BELIEF NETWORKS

E. V. Brezhnev, E. V. Broshevan, A. S. Karpenko

We propose the method of information security risk assessment (IS) for ICS, which takes into account the interaction between the IS states of its assets. The method is based on constructing the graph of the probabilistic risk model, which is based on Bayesian belief networks (BBN). Offeres illustrative example of the method for SCADA system. The developed method allows to evaluate the level of ICS to predict changes in IS levels of its interconnected assets, to generate scenarios of possible attacks and their consequences, and generate a variety of countermeasures to mitigate those risks. The method allows the efficient use of existing ICS resources to monitor risk assets and to solve the problem of diversion, taking into account the interaction between IS state.

Key words: BBN, ICS, risk assessment, incidents, information security.

Брежнев Евгений Витальевич – канд. техн. наук, доцент кафедры компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт». Харьков, Украина, e-mail: milestone@list.ru.

Брошеван Евгения Викторовна – студент кафедры компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: evgeniya.broshevan@live.ru.

Карпенко Андрей Сергеевич – студент кафедры компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: karpenkoandrew@yahoo.com.