УДК 004.056.53

РАСЧЕТ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

И. Р. ГАРИПОВ

ildar.garipov.92@mail.ru

ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ)

Аннотация. Приводится модель угроз нарушения информационной безопасности автоматизированной системы управления технологическим процессом в виде нечеткой когнитивной карты, а также метод численной оценки риска. Производятся расчеты численного значения риска нарушения информационной безопасности автоматизированной системы управления технологическим процессом.

Ключевые слова: автоматизированная система управления технологическим процессом, SCADA, PLC, OPC, ERP, MES, расчет рисков.

Автоматизированная система управления технологическим процессом (АСУ ТП)– это информационно-управляющая система, широко используемая в промышленности для автоматизации управления и сбора данных о технологическом процессе, повышения эффективности и качества производства [1].

Современная АСУ ТП представляет собой комплекс программно-аппаратных средств, реализующих сбор, обработку и хранение данных о процессах на производстве, позволяет управлять ими в режиме реального времени. На сегодняшний день в АСУ ТП активно используются широко распространенные операционные системы, протоколы информационного взаимодействия и различные технические решения, построенные на основе современной вычислительной техники. Вместе с большим количеством достоинств современные информационные технологии имеют и ряд недостатков в виде уязвимостей.

Промышленные сети зачастую входят в состав корпоративной информационной системы (КИС). Это обуславливается тем, что в рамках КИС разворачиваются системы планирования производства, учета ресурсов предприятия и выпускаемой продукции, такие как Enterprise Resource Planning (ERP) и Manufacturing Execution System (MES). Интеграция АСУ ТП в состав КИС дает возможность гибко управлять производством, вести учет выпускаемой продукции и затратных ресурсов предприятия. Использование общих каналов связи в рамках корпоративной сети позволяет оперативно обмениваться информацией между сегментами КИС и промышленной сетью.

Однако объединение промышленной сети и корпоративных сегментов приводит к обострению проблемы обеспечения информационной безопасности (ИБ).

Для поддержания приемлемого уровня защищенности информационных ресурсов предприятия необходимо гибкое управление ИБ. Также как для любой информационной системы, в процессе эксплуатации АСУ ТП необходимо периодическое проведение аудита ИБ.

Аудит ИБ – это систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в организации критериев информационной безопасности, а также допускающий возможность формирования профес-

сионального аудиторского суждения о состоянии информационной безопасности организации [2].

Моделирование угроз и расчет рисков ИБ являются методами экспертного аудита. Моделирование угроз позволяет специалисту по ИБ определить все возможные источники угроз, пути их реализации.

Необходимо определить все информационные активы в АСУ ТП, подлежащие защите, и источники угроз. В ходе исследований определены специфичные для АСУ ТП информационные активы, их местоположение, а также источники угроз. Ценность актива определяет собственник информации. Результаты представлены в табл. 1 и 2.

Таблица 1

Информационные активы, подлежащие защите

№	*Информационный актив*	*Местонахождение*	*Ценность актива*
1	Оперативные данные о технологическом процессе с датчиков	Сервер баз данных	0,1
2	Командная информация со SCADA-сервера	SCADA-сервера	0,3
3	Конфигурационная информация	Рабочая станция администратора безопасности	0,2
4	Программное обеспечение PLC	PLC	0,2
5	Программное обеспечение HMI	Рабочая станция Оператора	0,1
6	Программное обеспечение OPC	OPC сервер	0,1

Таблица 2

Возможные источники угроз нарушения информационной безопасности

№	*Источники угроз*	*Местонахождение*
1	Злоумышленник	За периметром КИС (Глобальная сеть)
2	Удаленный пользователь (авторизованный пользователь корпоративной сети)	КИС (корпоративная сеть (VPN канал связи))
3	Внутренний пользователь локальной сети	КИС (корпоративная сеть)
4	Внутренний авторизованный пользователь АСУ ТП	КИС (промышленная сеть)

На основе сведений (табл. 1, 2) и анализа инфраструктуры АСУ ТП [3] разрабатывается комплексная модель угроз нарушения ИБ в АСУ ТП в виде нечеткой когнитивной карты.

На рис. 1 представлена разработанная модель угроз в виде нечеткой когнитивной карты, которая позволяет визуализировать пути реализации атак в современной типовой АСУ ТП промышленного предприятия. Входными концептами в представленной модели являются источники угроз, выходными – компоненты АСУ ТП, содержащие информационные активы, подлежащие защите. Промежуточными концептами являются средства коммутации и защиты информации на пути реализации атаки.

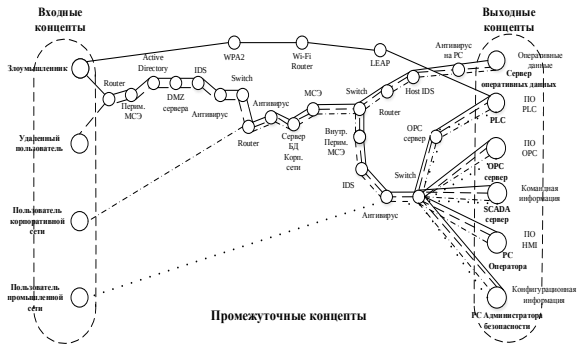

Рис. 1. Модель угроз нарушения ИБ в виде нечеткой когнитивной карты

На основе разработанной нечеткой когнитивной карты выполнить оценку риска нарушения информационной безопасности АСУ ТП по формуле:

$$R_{АСУТП} = \sum_i \frac{C_i}{C_\Sigma} P_i \ ,$$

где $R_{АСУТП}$ – численное значение уровня риска для АСУ ТП; $\frac{C_i}{C_\Sigma}$ – относительная стоимость информационного актива; P_i – результирующая вероятность угроз, исходящих от всех возможных источников угроз для *i*-го актива;

$$P_i = 1 - \prod_j (1 - P_{ji}),$$

где P_{ji} – вероятность угрозы от *j*-го источника к *i*-му активу;

$$P_{ji} = \max \prod_k w_{k\,ji},$$

где $w_{k_{ji}}$ – уровень уязвимости компонентов инфраструктуры и средств защиты; k – количество уязвимостей, учитываемых на пути распространения атаки.

Определим количество уязвимостей на пути реализации атаки от каждого источника к каждому активу.

Определим значения уязвимостей для каждого из промежуточных концептов на пути реализации атак. Значения уровней уязвимостей, представленные в табл. 3, были взяты из National vulnerability database (NVD) [4] и банка данных угроз безопасности информации ФСТЭК [5]. Значения уязвимостей для расчетов рисков необходимо нормировать. Данные, используемые в расчетах, представлены в табл. 3.

Таблица 3

Уязвимости компонентов инфраструктуры АСУ ТП

№	*Средства коммутации и защиты информации на пути распространения атаки*	*Обозначения уязвимости NVD и банк данных угроз безопасности информации*	*Нормированные значения уязвимостей*
1	Маршрутизатор (Router)	CVE-2018-10822	0,9
2	Коммутатор (Switch)	CVE-2018-5471	0,6
3	МСЭ	CVE-2018-0296	0,7
4	IDS	CVE-2018-6794, BDU:2018-00358	0,5
5	Active Directory	CVE-2018-1057	0,9
6	Антивирус	CVE-2018-0986	0,9
7	Host IDS	CVE-2018-0986, BDU:2018-00500	0,9
8	Антивирус на рабочей станции	CVE-2018-0986, BDU:2018-00500	0,9
9	Сервер баз данных (внешней подсети промышленного предприятия)	CVE-2018-8589	0,8
10	Сервер баз данных (экранированная подсеть предприятия)	CVE-2018-8589	0,8
11	Рабочая станция оператора (Системное ПО)	CVE-2018-8589	0,8
12	SCADA	CVE-2018-13799	0,9
13	OPC	CVE-2018-12086	0,7
14	PLC	CVE-2018-4850	0,7
15	WPA 2	CVE-2017-13077	0,7
16	Wi-Fi router	CVE-2017-13077	0,7
17	РС администратора безопасности (Системное ПО)	CVE-2018-8589	0,8

Окончание табл. 3

Расчеты показали, что значение риска нарушения ИБ АСУ ТП с выбранными в примере средствами защиты составило 23 %.

В данной работе была предложена модель угроз информационной безопасности в виде когнитивной карты. Определены компоненты и информационные активы АСУ ТП, подлежащие защите. Обнаружены возможные источники атак на важные объекты. Определены уязвимости IT-инфраструктуры. Приведены результаты расчетов численной оценки риска нарушения ИБ АСУ ТП.

Целью анализа рисков в АСУ ТП является снижение риска до приемлемого уровня. Величина риска может быть снижена

путем установки дополнительных средств защиты на возможных путях проникновения атак или замены защитных механизмов.

СПИСОК ЛИТЕРАТУРЫ

1. **I. Mashkina**, I. Garipov, Development of Protection Object Model – Industrial Control System Using System Analysis. URL: https://ieeexplore.ieee.org/document/8501733 (дата обращения 06. 01.2019).

2. **ГОСТ** Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

3. **I. Mashkina**, I. Garipov, Threats Modeling and Quantitative Risk Analysis in Industrial Control Systems. URL: https://ieeexplore.ieee.org/document/8501694 (дата обращения 06. 01.2019).

4. **National** Vulnerability Database. URL: https://nvd.nist.gov/ (дата обращения 06. 01.2019).

5. **Банк** данных угроз безопасности информации. URL: http://bdu.fstec.ru/ubi (дата обращения 06. 01.2019).

ОБ АВТОРЕ

ГАРИПОВ Ильдар Рамилевич, аспирант. каф. ВТиЗИ.

METADATA

Title: Calculation of risk of violation information security ICS
Authors: I. R. Garipov
Affiliation:
Ufa State Aviation Technical University (UGATU), Russia.
Email: ildar.garipov.92@mail.ru
Language: Russian.
Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), no. 1 (20), pp. 41-44, 2019**.** ISSN 2225-9309 (Print).
Abstract: This article presents a model of information security threats in an Industrial Control System (ICS) in the form of a fuzzy cognitive map, as well as a method of quantitative risk evaluation. The quantitative value of the information security risk of the ICS has been calculated in the paper.
Key words: steam turbine, power station, economy, power generation, fuel consumption, outdoor temperature, electrical energy, operation, efficiency, energy performance CHP.
About author:
GARIPOV, Ildar Ramilevich., postgraduate 4 year, Ufa state aviation technical University