Методика оценки рисков кибербезопасности АСУ ТП промышленного объекта

В. И. Васильев
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: vasilyev@ugatu.ac.ru

А. М. Вульфин
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: vulfin.alexey@yandex.ru

К. И. Муслимова
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: karinamuslimova@mail.ru

Аннотация[1]

Целью работы является разработка формализованной методики комплексной оценки выполнения требований к обеспечению защиты информации в автоматизированной системе с применением метода нечеткого логического вывода и экспертных оценок. Предложена методика качественной и количественной оценки рисков кибербезопасности АСУ ТП промышленного объекта. Рассмотрена зональная и трактовая модель промышленного объекта на основе стандарта ГОСТ Р МЭК 62443. На примере конкретной АСУ ТП определен перечень внешних и внутренних угроз, а также перечень уязвимостей и последствий от воздействия угроз. Предложена процедура определения уровня значимости (критичности) обрабатываемой информации на основе системы нечетких правил (продукций) с учетом степени возможного ущерба от нарушения целостности, доступности или конфиденциальности информации.

Ключевые слова: кибербезопасность; АСУ ТП; угрозы; ГОСТ Р 62443; приказ ФСТЭК №31.

Труды Седьмой всероссийской научной конференции "Информационные технологии интеллектуальной поддержки принятия решений", 28-30 мая, Уфа-Ставрополь, Ханты-Мансийск, Россия, 2019

1. Введение

Несмотря на актуальность проблемы защищенности АСУ ТП, понятие «кибербезопасность» в России вошло в обиход сравнительно недавно. В 2014 году был принят ГОСТ Р 56205-2014 (его прототип – стандарт IEC/TC 62443-1-1:2009), в котором кибербезопасность определена как «действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразовании, рассекречивании, потери прибыли, или повреждении критических систем или информационных объектов» [1].

Основные документы, определяющие на сегодняшний день рекомендуемые подходы к обеспечению кибербезопасности в Российской Федерации: Приказ ФСТЭК России от 14.03.2014 №31 [2]; Федеральный закон от 26.07.2017 № 187-ФЗ [3]; Приказ ФСТЭК России от 25.12.2017 №239 [4]; ГОСТ Р 56205-2014 IEC 62443-1-1:2009 [1]; ГОСТ Р МЭК 62443-2-1-2015 (IEC 62443-2) [5]; ГОСТ Р 56498 IEC 62443-3-3-2016 [6].

При оценке рисков кибербезопаности необходимо руководствоваться требованиями приказа ФСТЭК №31, в котором описывается последовательность отнесения АСУ ТП к одному из трех классов защищенности. Каждому классу соответствуют определенные меры защиты. Необходимо оценить, насколько выполняются данные требования на промышленном объекте.

В стандартах серии 62443 подробно описываются требования к системной безопасности и уровни безопасности, вопросы, которые необходимо учесть при оценке рисков кибербезопасности АСУ ТП. На основе данных рекомендаций и концептуальных

моделей в работе предложен подход к оценке рисков, разработаны модели угроз и уязвимостей для промышленного объекта.

2. Определение актуальных угроз кибербезопасности АСУ ТП на основе стандартов серии 62443

Исходя из специфики функционирования отдельных сегментов промышленного объекта (относящихся к бизнесу, техническим средствам, производственным объектам и системе в целом), в соответствии с зональной моделью стандартов серии 62443 были выделены следующие зоны, представленные на рисунке 1:

- Сеть управления (Control network);
- Полевая сеть (Field network).

Актуальные уязвимости для зон:

1. Уязвимости для сети управления:

- Возможность атаки перебором из корпоративной беспроводной сети;
- Доверчивые сотрудники/Недостаточно обученный персонал;
- Антивирусная защита.

2. Уязвимости промышленной сети (полевой сети):

- Система не установила должного ограничения потока данных;
- Случайный сбой оборудования;
- Недовольный работник / подрядчик.

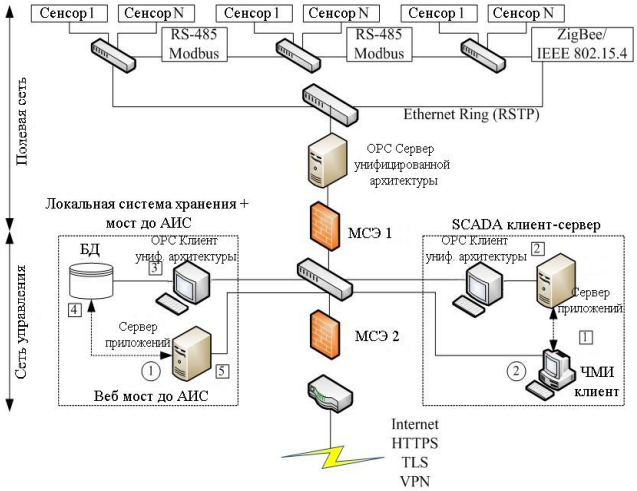

Рис.1. Подсистема сбора и хранения данных на станциях обслуживания летательных аппаратов

К данным уязвимостям применимы следующие угрозы кибербезопасности:

- НСД к серверу приложений через межсетевой экран промышленно-корпоративной ДМЗ;
- Фишинг;
- Расширение привилегий;
- Непреднамеренное попадание в систему управления вредоносного ПО через HMI;
- Атака «отказ в обслуживании»;
- Случайный или непредумышленный доступ;
- Сбой сетевого устройства, вызывающий сетевой шторм, влияющий на связь системы.

Перечень угроз составлен с учетом следующих классификационных признаков (характеристик):

- Источник угрозы;
- Уязвимость;
- Сценарий реализации угрозы;
- Последствия воздействия угрозы.

Отдельно учитывалось происхождение источника угроз – внутренние и внешние угрозы.

Наиболее вероятные нарушители кибербезопасности:

- Недовольные работники или подрядчики, которые повреждают системы или крадут информацию из чувства мести или для получения прибыли;
- Благонамеренные сотрудники, которые случайно допустили ошибку при внесении изменений в контроллер или работающее оборудование;
- Работники, которые нарушают политики качества, безопасности или процедуры удовлетворения других насущных потребностей (например, производственные цели);
- Хакеры, реализующие для проникновения в компьютерные сети ненаправленные (вирусы и "черви") или направленные атаки (взлом) с целью кражи или уничтожения информации, или нарушения деятельности организации;
- Профессиональные воры (в том числе организованная преступность), которые осуществляют кражу информации для продажи;
- Террористы, как правило движимые политическими убеждениями, для которых кибератаки имеют потенциал недорогих, низкорискованных, но мощных атак, в особенности, когда они связаны с координированными физическими атаками.

3. Методика оценки рисков кибербезопасности АСУ ТП

Перед выполнением оценки рисков необходимо определить конкретные требования к безопасности, с учетом требований приказа ФСТЭК № 31. После установления уровня значимости (критичности) информации и класса защищённости АСУ ТП

необходима оценка соответствия реального состояния ИБ на объекте этим требования (аудит ИБ).

Приказ ФСТЭК № 31 содержит 21 группу мер защиты информации (см. таблицу 1), каждая из которых включает в себя различное количество (от 3 до 31) конкретных мер защиты.

Таблица 1. Исследование мер защиты информации

№ группы мер i	Группы мер защиты информации	Число мер защиты (n_i)	Показатель EV_i, %	Показатель NE_i
1	2	3	4	5
1	Идентификация и аутентификация субъектов доступа и объектов доступа	8		
2	Управление доступом субъектов доступа к объектам доступа	18		
3	Ограничение программной среды	5		
4	Защита машинных носителей информации	9		
5	Регистрация событий безопасности	9		
6	Антивирусная защита	3		
7	Обнаружение вторжений	3		
8	Контроль (анализ) защищенности информации	6		
9	Обеспечение целостности	9		
10	Обеспечение доступности	8		
11	Защита среды виртуализации	11		
12	Защита технических средств	6		
13	Защита автоматизированной системы и ее компонентов	31		
14	Обеспечение безопасной разработки программного обеспечения	7		
15	Управление обновлениями программного обеспечения	4		
16	Планирование мероприятий по обновлению защиты информации	4		
17	Обеспечение действий в нештатных (непредвиденных) ситуациях	6		
18	Информирование и обучение персонала	4		
19	Анализ угроз безопасности информации и рисков от их реализации	4		
20	Выявление инцидентов и реагирование на них	7		
21	Управление конфигурацией автоматизированной системы управления и ее системы защиты	6		

Обозначим через M_{ij} частный показатель полноты использования j-ой меры защиты в i-ой группе мер, где M_{ij} принимает значение 0, если соответствующая мера защиты не применяется, 0,5 - если данная мера защиты используется частично и 1 - если данная мера защиты используется в полном объеме; n_i - количество мер защиты в i-ой группе, рекомендованных для данного класса защищенности АСУ ТП. Каждой i-ой группе мер защиты можно присвоить групповой показатель полноты использования EV_i мер защиты из базового набора мер защиты, выраженный в процентах (формула 1), и абсолютный показатель количества N_i неиспользованных или частично использованных мер защиты из рекомендованного базового набора NE_i (формула 2):

$$EV_i = \left(\frac{1}{n_i} \sum_{j=1}^{n_i} M_{ij} \right) \cdot 100\% \quad (1)$$

$$NE_i = n_i - \sum_{j=1}^{n_i} unit\left(M_{ij}\right) \quad (2)$$

где функция unit(M_{ij}) равна 1, если $M_{ij} = 1$, и 0, если $M_{ij} = 0$ или 0,5 [7].

Предложена [8] методика качественной оценки рисков кибербезопасности АСУ ТП, основанная на построении системы нечетких продукционных правил. При этом в качестве базовой используется трехфакторная формула риска: Риск (ущерб) = Угроза * Уязвимость * Информационный материальный ресурс, где Угроза * Уязвимость = Степень реализации угрозы (опасность угрозы).

Нечеткие понятия на основе знаний экспертов формализуются в данном случае в форме нечетких продукций. Предполагается, что при оценке риска эксперт может ввести для каждой угрозы значения вероятностей возникновения угрозы и уязвимости, а также значение стоимости информационного материального ресурса (Таблицы 2,3). В этих таблицах приведены лингвистические значения (термы) опасности угрозы и риска от воздействия угрозы: S – Small, M- Medium, L-Large.

Таблица 2 Определение опасности угрозы

		Уязвимость		
Угроза		**S**	**M**	**L**
	S	S	S	M
	M	S	M	L
	L	M	L	L

Таблица 3 Определение значения риска

		Стоимость ресурса		
Опасность угрозы		**S**	**M**	**L**
	S	S	S	M
	M	S	M	L
	L	M	L	L

Для количественной оценки рисков также можно использовать методику, основанную на построении нечеткой нейронной сети ANFIS (Рисунок 2) [9].

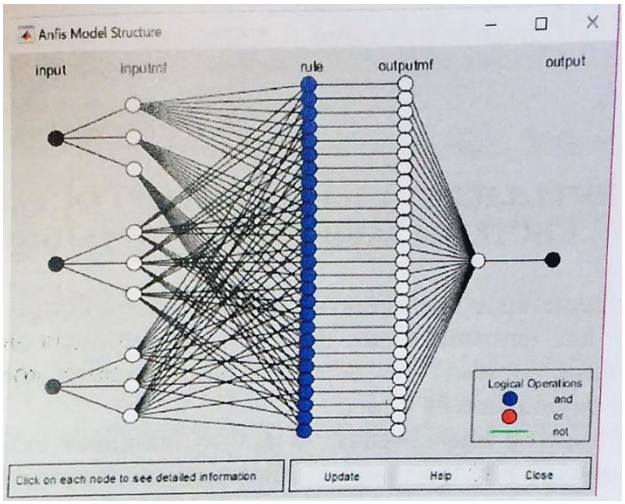

Рис.2. Структура нечеткой нейронной сети

На входы нейроннной сети подаются значения вероятностей угрозы, уязвимости, стоимости ресурса. Используя алгоритм нечеткого вывода Мамдани, можно получить количественную оценку риска кибербезопасности, т.е. величину ущерба для соответствующего ресурса.

Для оценки риска выделенной зоны безопасности рекомендуется оценить величину ущерба от реализации каждой угрозы в зоне, полученные результаты просуммировать. Используя данный подход, можно получить количественную оценку рисков как для конкретной зоны безопасности, так и для всего промышленного объекта.

Посредством выполнения оценки рисков АСУ ТП и установления на ее основе факта того, выполняются ли конкретные требования к ее безопасности, определяются целевые (желаемые) уровни зон безопасности (SL-T) [6]. Достигнутые уровни безопасности SL-A - это фактические уровни безопасности для анализируемой системы. Потенциальные уровни безопасности (SL-C) - это уровни безопасности, реально обеспечивающиеся при корректно сконфигурированных компонентах или системах. При разработке системы безопасности АСУ ТП, если SL-C < SL-T, должны быть предусмотрены дополнительные компенсационные контрмеры, с целью обеспечения соответствия SL-T. После завершения реализации проекта проверяется выполнение условия SL-A= SL -T.

В данной работе для всех зон применяется потенциальный уровень безопасности SL (SL-C) 3, к которому предъявляются следующие требования:

- управление идентификацией и аутентификацией (IAC);
- контроль использования (UC);
- целостность системы (SI);
- конфиденциальность данных (DC);
- ограничение потока данных (RDF);
- своевременный отклик на события (TRE);
- работоспособность и доступность ресурсов (RA).

Использование предложенной методики определения актуальных угроз позволяет дать комплексную оценку рисков кибербезопасности АСУ ТП, и в конечном итоге – возможность принятия обоснованных решений по выбору эффективных защитных мер, и как следствие, обеспечение заданного (целевого) уровня безопасности промышленного объекта.

Данная работа поддержана грантом РФФИ №17-07-00351 А.

4. Заключение

Оценка рисков кибербезопасности должна базироваться на соответствии требованиям нормативных документов, в частности приказа ФСТЭК №31 и стандартов серии 62443.

Перед выполнением оценки рисков необходимо определить конкретные требования к безопасности, в частности соответствие требованиям приказа ФСТЭК № 31.

В соответствии с приказом ФСТЭК №31, определяются уровень значимости (критичности) информации и класс защищённости АСУ ТП. Затем проводится оценка соответствия реального состояния

информационной безопасности на объекте этим требованиям.

Для количественной оценки рисков возможно использование нечеткой нейронной сети, на входы которой подаются значения вероятностей угрозы, уязвимости, стоимости ресурса, определяемые экспертом.

Актуальные угрозы и уязвимости определяются на основе стандартов серии 62443 и с учетом специфики промышленного объекта.

Список используемых источников

1. ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200114169 (дата обращения 16.10.2018).
2. Приказ ФСТЭК России от 14.03.2014 № 31 [Электронный ресурс]. – Режим доступа: https://www.law.ru/npd/doc/docid/420397221/modid/99 (дата обращения 16.10.2018).
3. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW _220885/ (дата обращения 16.10.2018).
4. Приказ ФСТЭК от 25 декабря 2017 г. № 239 “Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации” [Электронный ресурс]. – Режим доступа: http://www.garant.ru/products/ipo/prime/doc/71801880/ (дата обращения 16.10.2018).
5. ГОСТ Р МЭК 62443-2-1-2015 (IEC 62443-2) Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200121982 (дата обращения 16.10.2018).
6. ГОСТ Р 56498 IEC 62443-3-3-2016 Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru /document/1200135801 (дата обращения 16.10.2018).
7. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д. Комплексная оценка выполнения требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами. [Статья из сборника] / «Инфокоммуникационные технологии» Том 15, № 4, 2017. – с. 319-325.
8. Васильев В. И., Кучкарова Н.В., Муслимова К.И. Методика определения актуальных угроз кибербезопасности АСУ ТП на основе стандарта ГОСТ Р 62443. [Статья из сборника] / Сборник избранных статей по материалам научных конференций ГНИИ «Нацразвитие» – Санкт-Петербург, 2018. – с. 122-126.
9. Кириллова А.Д., Васильев В.И. Применение нечеткой нейронной сети для оценки рисков информационной безопасности АСУ ТП. Проблемы информационной безопасности, / Материалы VII Всеросс. Заочной Интернет-конференции, 20-21 февр. 2018 г. – Ростов-на-Дону. – Издательство ООО «Азов Принт», 2018. – с. 138-142.