УДК 004.052

Вестник УрФО № 2(36) / 2020, с. 56–60

Афанасьева М. В., Абзалутдинов Д. Р., Бараков К. Я. DOI: 10.14529/secur200209

ПРИНЦИПЫ ПОСТРОЕНИЯ МОДЕЛИ НАДЕЖНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ АСУ ТП

В статье рассмотрена возможность применения теории надежности технических систем для количественной оценки уровня защиты системой управления кибербезопасностью АСУ ТП. Построена модель надежности и определена функция надежности для каждого компонента подсистемы. Также приведены аналитические выражения для расчета вероятности безотказной работы системы управления кибербезопасностью АСУ ТП в целом, построена модель надежности системы с учетом её подсистем.

Ключевые слова: *модель надежности, система управления кибербезопасностью, функция надежности, последовательно-параллельная схема.*

Afanaseva M. V., Abzalutdinov D. R., Barakov K. Y.

CYBERSECURITY MANAGEMENT OF INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS: PRINCIPLES OF RELIABILITY MODEL BUILDING

The article considers the possibility of applying the reliability engineering theory for the quantification of cyber security level of industrial automation and control systems security. The reliability model was built and the reliability function for each component of the subsystem was determined. Analytical expressions for the cybersecurity management system uptime probability calculation are also given, and a system reliability model was built taking into account its subsystems.

Keywords: *reliability model, cybersecurity management system, reliability function, serial-parallel circuit.*

Рис. 1. Структурная схема CSMS

В настоящее время при анализе эффективности систем защиты информации (СЗИ) в рамках оценки защищенности информации мало рассматривается оценка надежности защиты информации в связи с отсутствием моделей надежности, учитывающих специфику СЗИ и согласующихся с подходами, построенных на классической теории надежности технических систем [1]. Оценивая надежность защищенности АСУ ТП, необходимо учитывать факт, что безопасность АСУ ТП не сводится к обеспечению информационной безопасности (ИБ), т.е. обеспечению конфиденциальности собираемой, обрабатываемой и передаваемой информации [2–3]. Безопасность АСУ ТП должна заключаться прежде всего в обеспечении непрерывности и целостности самого ТП [3]. Эта особенность еще более усложняет анализ надежности защищенности АСУ ТП, поэтому вопрос о разработке модели надежности защиты промышленных объектов является важной и актуальной задачей.

Согласно ГОСТ Р МЭК 62443-2-1—2015 система управления кибербезопасностью (CSMS) АСУ ТП включает в себя следующие элементы, представленные на рис. 1.

Данная схема соединения компонентов CSMS имеет сложную комбинированную структуру, поэтому целесообразно предварительно произвести декомпозицию системы, разбив ее на простые подсистемы, которые, в свою очередь, так же разбить на более простые квазиэлементы.

Модель надежности CSMS представлен на рис. 2.

Данная структура имеет вид последовательного соединения, которое в теории надежности используется тогда, когда отказ одного элемента приводит к отказу всей системы [5]. Выбор такого типа соединения обусловлен следующими тремя ситуациями. Без проведения анализа рисков кибератак CSMS (отказ подсистемы «Анализ рисков») организация не сможет убедить руководство выделить средства на создание CSMS, и, следовательно, нечего будет совершенствовать, и наступит отказ всей системы CSMS. Также отказ CSMS наступит, если не будут приниматься меры по устранению рисков. И, наконец, без контроля и совершенствования CSMS будет неэффективной для защиты от постоянно появляющихся кибератак, и в итоге наступит отказ всей системы.

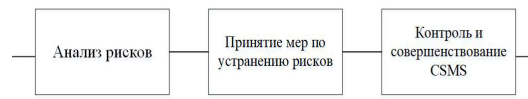

Рис. 2. Модель надежности CSMS

Функция надежности CSMSпринимает следующий вид:

$$P_{CSMS}(t) = P_{AP}(t) \cdot P_{ПМ}(t) \cdot P_{КС}(t), \quad (1)$$

где $P_{AP}(t)$– вероятность безотказной работы (ВБР) подсистемы «Анализ рисков», %;

$P_{ПМ}(t)$– ВБР подсистемы «Принятие мер по устранению рисков», %;

$P_{КС}(t)$– ВБР подсистемы «Контроль и совершенствование CSMS», %;

t – время, с.

Далее оценим надежность каждой подсистемы отдельно также применяя декомпозицию.

Подсистема «Анализ рисков»

Цель данной подсистемы – идентифицировать и документально описать уникальные потребности организации для устранения рисков кибератак в отношении АСУ ТП и определить комплекс кибер-рисков АСУ ТП, которые угрожают организации, и оценить вероятность и уровень серьезности таких рисков. Отсюда можно сделать вывод, что компоненты анализов рисков кибербезопасности, как одного из компонентов CSMS в целом на схеме ее надежности должны быть соединены последовательно (рис. 3).

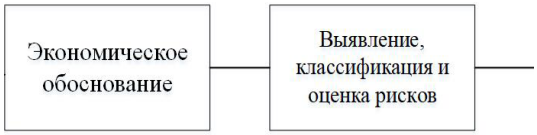

Рис. 3. Модель надежности подсистемы «Анализ рисков»

Функция надежности:

$$P_{АР}(t) = P_{ЭО}(t) \cdot P_{Р}(t), \quad (2)$$

где $P_{ЭО}(t)$ – ВБР компонента «Экономическое обоснование», %;

$P_{Р}(t)$– ВБР компонента «Выявление, классификация и оценка рисков», %;

Подсистема «Принятие мер по устранению рисков»

Рассмотрим причины и механизмы возникновения отказа в данной подсистеме.

Применительно к компоненту «Политика, организация и понимание необходимости безопасности»:

– не разработан формальный письменный документ с описанием сферы применения для программы обеспечения кибербезопасности;

– не организованы структурные единицы, ответственные за управление, проведение и оценку общей кибербезопасности объектов АСУ ТП;

– не разработана и не внедрена программа обучения по работе с системой ИБ;

– персонал не прошел первоначальное и периодическое обучение по вопросам работы с правильными процессами безопасности и правильному использованию объектов обработки информации, а также отсутствие процедуры аттестации программы обучения;

– не разработаны политика и процедуры безопасности и не доведены до персонала.

Применительно к компоненту «Избранные контрмеры по обеспечению безопасности»:

– не установлена политика в области безопасности персонала;

– не реализована физическая безопасность и защита от внешних воздействий;

Применительно к компоненту «Внедрение»:

– не принята схема управления рисками;

– не применен общий комплекс контрмер, направленных на физические риски и риски для информационной безопасности при идентификации определенного риска.

Так как при выходе из строя хотя бы одной из составляющих частей данной подсистемы вероятность кибератаки увеличится, но не приведет к отказу всей подсистемы в целом, и каждая часть подсистемы может функционировать вне зависимости от других, обеспечивая требуемый уровень защиты, поэтому все части рассмотренной подсистемы должны быть соединены параллельно (рис. 4).

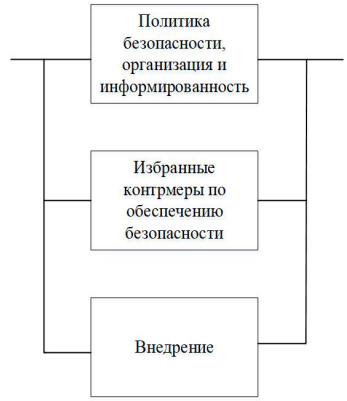

Рис. 4. Модель надежности подсистемы «Принятие мер по устранению рисков»

Функция надежности:

$$P_{ПМ}(t) = 1-(1-P_{ПБ}(t)) \cdot (1-P_{ИК}(t)) \cdot (1-P_{В}(t)), \quad (3)$$

где $P_{ПБ}(t)$– ВБР компонента «Политика безопасности»;

$P_{ИК}(t)$– ВБР компонента «Избранные контрмеры»;

$P_{В}(t)$ – ВБР компонента «Внедрение».

Подсистема «Контроль и совершенствование CSMS»

Данная подсистема обеспечивает соответствие CSMS, которое означает, что организация придерживается официальной политики, своевременно выполняет процедуры и составляет отчеты для последующего анализа. Также в рамках этой подсистемы обеспечивается анализ, совершенствование и поддержание CSMS. Отказ одного из компонентов не приведет к отказу подсистемы, следовательно, компоненты представляют собой параллельное соединение (рис. 5).

Рис. 5. Модель надежности подсистемы «Контроль и совершенствование CSMS»

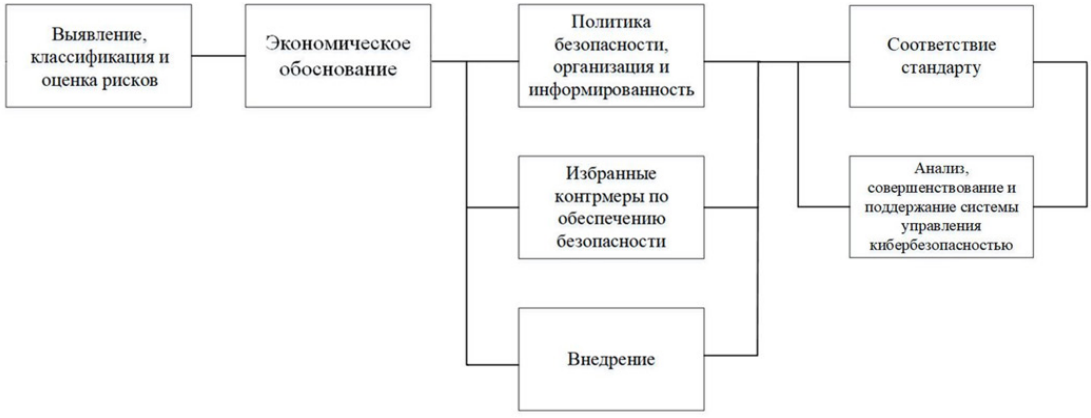

Рис. 6. Модель надежности CSMS с учетом структур ее подсистем

Функция надежности:

$P_{КС}(t) = 1-(1-P_{СС}(t)) \cdot (1-P_{АСПК}(t))$, (4)

где $P_{СС}(t)$ – ВБР компонента «Соответствие стандарту»;

$P_{АСПК}(t)$ – ВБР компонента «Анализ, совершенствование и поддержание системы управления кибербезопасностью».

Подставим в модель надежности CSMS модели надежности подсистем «Анализ рисков», «Принятие мер по устранению рисков» и «Контроль и совершенствование CSMS», чтобы получить модель надежности CSMS с учетом структур ее подсистем (рис. 6).

Подставим в (1) функции надежности (2), (3) и (4), чтобы получить функцию надежности CSMS с учетом структур ее подсистем:

$$P_{CSMS}(t) = P_{ЭО}(t) \cdot P_{Р}(t) \cdot P_{ПМ}(t) \cdot P_{КС}(t) \cdot [1-(1-P_{ПБ}(t)) \cdot (1-P_{ИК}(t)) \cdot (1-P_{В}(t))] \cdot [1-(1-P_{СС}(t)) \cdot (1-P_{АСПК}(t))].$$

С помощью полученной функции надежности CSMS можно оценивать эффективность мер защиты АСУ ТП и выявлять наиболее ненадежные компоненты системы. Таким образом, полученная информация о надежности системы в данной момент времени дополнит общую картину защищенности предприятия и позволит принять необходимые меры для повышения уровня защиты.

Литература

1. Булгаков О.М., Стукалов В.В., Кучмасов Е.А. Принципы построения модели надежности организационного компонента системы защиты информации объекта информатизации//Вестник Воронежского института МВД России. -2013. - № 2. - С.145–155.

2. Ярушевский Д. Кибербезопасность АСУ ТП – что это и зачем? [Электронный ресурс]. URL: https://www.dialognauka.ru/press-center/article/13226 (дата обращения 9.10.2019).

3. Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии//Международная конференция «Наука. Исследования. Практика». – 2019. – С. 341–345.

4. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Прогнозирование локальных и внешних угроз на информационные серверы предприятия//Актуальные проблемы современной науки, техники и образования. -2017. -Т. 1. С. 217–220.

5. Афанасьева М.В. Лабораторный практикум по курсу «Теоретические основы обеспечения надежности систем автоматизации и модулей мехатронных систем»: лабораторный практикум – Магнитогорск, 2019.

6. ГОСТ Р МЭК 62443-2-1-2015.

References

1. Bulgakov O.M., Stukalov V.V., Kuchmasov Ye.A. Printsipy postroyeniya modeli nadezhnosti organizatsionnogo komponenta sistemy zashchity informatsii ob»yekta informatizatsii//Vestnik Voronezhskogo instituta MVD Rossii. -2013. -№ 2. -S. 145–155.

2. Yarushevskiy D. Kiberbezopasnost' ASU TP – chto eto i zachem? [Elektronnyy resurs]. URL: https://www.dialognauka.ru/press-center/article/13226 (data obrashcheniya 9.10.2019).

3. Mikhaylova U.V., Bykova T.V. Audit informatsionnoy bezopasnosti na predpriyatii//Mezhdunarodnaya konferentsiya «Nauka. Issledovaniya. Praktika». – 2019. – S. 341–345.

4. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Prognozirovaniye lokal'nykh i vneshnikh ugroz na informatsionnyye servery predpriyatiya//Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. -2017. -T. 1. S. 217–220.

5. Afanas'yeva M. V. Laboratornyy praktikum po kursu «Teoreticheskiye osnovy obespecheniya nadezhnosti sistem avtomatizatsii i moduley mekhatronnykh sistem»: laboratornyy praktikum – Magnitogorsk, 2019.

6. GOST R MEK 62443-2-1-2015.

АФАНАСЬЕВА Маргарита Владимировна, старший преподаватель кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, Россия, Челябинская область, г. Магнитогорск, пр. Ленина, 38. E-mail: nansy_stokli@mail.ru

АБЗАЛУТДИНОВ Данил Римович, студент второго курса Института энергетики и автоматизированных систем по направлению подготовки Информационная безопасность автоматизированных систем, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, Россия, Челябинская область, г. Магнитогорск, пр. Ленина, 38. E-mail: abz-dan@yandex.ru

БАРАКОВ Камил Ялилевич, студент второго курса Института энергетики и автоматизированных систем по направлению подготовки Информационная безопасность автоматизированных систем, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, Россия, Челябинская область, г. Магнитогорск, пр. Ленина, 38. E-mail: kamil.barakov@gmail.com

AFANASEVA Margarita, Senior lecturer at theDepartment of Computer Science and Cyber security, Nosov Magnitogorsk State Technical University. 455000, Russia, Chelyabinsk Region, Magnitogorsk, 38 Lenin avenue. E-mail: nansy_stokli@mail.ru

ABZALUTDINOV Danil, second-year student at the Power Engineering and Automated Systems Institute, Department of Computer Science and Cyber security, Nosov Magnitogorsk State Technical University. 455000, Russia, Chelyabinsk Region, Magnitogorsk, 38 Lenin avenue. E-mail: abz-dan@yandex.ru

BARAKOV Kamil, second-year student at the Power Engineering and Automated Systems Institute, Department of Computer Science and Cyber security, Nosov Magnitogorsk State Technical University. 455000, Russia, Chelyabinsk Region, Magnitogorsk, 38 Lenin avenue. E-mail: kamil.barakov@gmail.com