АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

УДК 004.056.53

Вестник УрФО № 3(41) / 2021, с. 57–64

Баранкова И.И., Афанасьева М.В., Федорова А.Р.

DOI: 10.14529/secur210307

МОДЕЛЬ ЗРЕЛОСТИ БЕЗОПАСНОСТИ АСУ ТП ДОМЕННОЙ ПЕЧИ №10 ПАО «ММК»

В статье рассматриваются понятия зрелости безопасности, модель и целевой профиль зрелости безопасности, приводятся требования к построению модели зрелости безопасности и шкала оценки уровней полноты практик безопасности. В ходе работы представляется текущий профиль безопасности АСУ ТП доменной печи, определяется целевой профиль зрелости безопасности по уровням полноты, а также дается оценка наиболее значимым практикам модели зрелости безопасности. Завершающим этапом работы является анализ текущего и целевого профилей безопасности для выявления пробелов.

Ключевые слова: *информационная безопасность, АСУ ТП, модель зрелости безопасности, целевой профиль зрелости безопасности.*

Barankova I.I., Afanasyeva M.V., Fedorova A.R.

MMK PJSC BLAST FURNACE NO. 10 AUTOMATED PROCESS CONTROL SYSTEM SAFETY MATURITY MODEL

The article discusses the concepts of security maturity, the model and the target profile of security maturity, the requirements for building a model of security maturity and a scale for assessing the levels of completeness of security practices. In the course of the work, the current safety profile of the blast furnace automated process control system is presented, the target safety maturity profile is determined by completeness levels, and the most significant practices of the safety maturity model are evaluated. The final stage of the work is the analysis of the current and target security profiles to identify gaps.

Keywords: *information security, automated control system, security maturity model, target profile of security maturity.*

Нарастающая сложность технологий, применяемых в промышленных системах, расширяет поверхность атак, создавая новые риски там, где раньше использовались некомпьютеризированные подходы или отсутствовало постоянное сетевое взаимодействие с внешним миром. Поэтому одной из основных задач в эпоху цифровизации на промышленных предприятиях является разработка стратегии защиты от киберугроз, которая проходит следующие стадии: проектирование, разработка, интеграция, использование и сопровождение. Участие в вышеперечисленных процессах сопровождается наличием большого количества участников и оценка рисков, связанных с атаками, у всех осуществляется по-разному. Существует две точки зрения в отношении безопасности для бизнеса – увеличение времени выхода на рынок или безопасный продукт, у которого есть преимущество на рынке. При автоматизации технологических процессов, производители информационных продуктов перекладывают свою ответственность на клиентов под предлогом того, что продукт должен быть изолирован от внешнего воздействия, что вовсе не может быть достижимо. Предприятия же аналогичным образом зачастую не могут полностью пользоваться продуктом автоматизации с точки зрения обеспечения безопасности без подтверждения со стороны производителя продукта [1]. Таким образом, важной и актуальной задачей на данный момент является выработка стратегически правильного подхода к управлению уязвимостями, грамотного инвестирования в механизмы безопасности, отвечающие требованиям предприятия, без чрезмерных вложений в ненужных механизмах безопасности, а также предоставить концептуальную основу для помощи в выборе и реализации соответствующих меры безопасности из бесчисленного множества вариантов.

Так как не все системы требуют одинаковой силы защитных механизмов или процедур, чтобы соответствовать их требованиям безопасности, то организационное руководство определяет приоритеты, которые движут процесс повышения безопасности, что позволяет механизмам и процедурам соответствовать цели организации, не выходя за рамки необходимого. Реализации механизмов безопасности считаются зрелыми, если ожидается, что они будут эффективны в достижении этих целей. Соответствие механизмов безопасности достижению поставленных целей, т.е. зрелость, определяется не их объективной силой. Следовательно, зрелость безопасности – это мера понимания текущего уровня безопасности, ее необходимости, преимущества и стоимости ее поддержки.

Модель зрелости безопасности представляет собой иерархию практик обеспечения безопасности, сгруппированные по ожидаемому эффекту от их применения, описанные в [2]. Для упрощения понимания модели зрелости на самом верхнем уровне практик они объединены в так называемые домены.

Три верхнеуровневых домена безопасности включают:

1. управление безопасностью и организационные меры (Управление);

2. обеспечение безопасности в силу конструкции (Внедрение);

3. укрепление безопасности (Укрепление).

Приоритет того или иного домена перед другим определяется потребностями бизнеса и особенностями системы.

На втором уровне каждый из доменов делится на три поддомена, которые классифицируют практики безопасности в соответствии с проблемой, на решение которой они нацелены. И наконец, каждый поддомен ссылается на 2 практики, каждая из которых решает некоторую задачу (рисунок 1).

Существуют два ортогональных аспекта оценки зрелости: полнота и специфичность. Полнота отражает степень глубины, последовательности и обеспечение мер безопасности, которые поддерживают домены зрелости безопасности, субдомены или практики. Например, более высокий уровень полноты моделирования угроз подразумевает большее автоматизированный системный и разносторонний подход. Специфика отражает степень соответствия отрасли или системным потребностям. Это отражает степень настройки мер безопасности, поддерживающих домены зрелости безопасности, поддомены или практики. Такие настройки обычно требуются для устранения отраслевых или системных ограничений АСУ ТП. Полнота и специфичность помогают оценивать и расставлять приоритеты в практике зрелости безопасности [3,4].

Полнота реализации практики оценивается по следующей шкале:

– нулевой уровень (уровень 0): нет единого понимания того, как применяется практи-

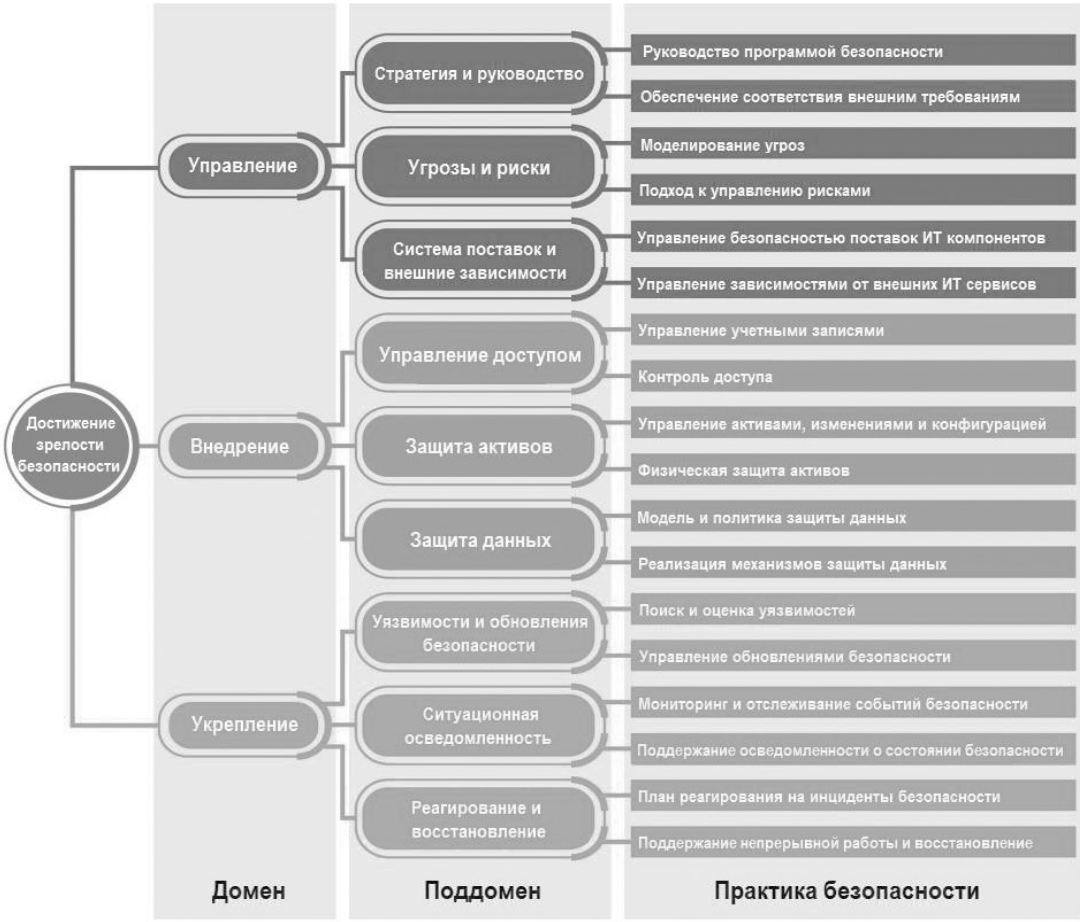

Рис. 1. Иерархия доменов, субдоменов и практик в модели зрелости безопасности

ка безопасности, и нет соответствующих требований, которые необходимо реализовать

– минимальный уровень (уровень 1): соблюдены минимальные требования практики безопасности.

– специальный уровень (уровень 2): требования к практике охватывают основные варианты использования и общеизвестные инциденты безопасности в аналогичных средах. Требования повышают точность и уровень детализации для рассматриваемой среды.

– постоянный уровень (уровень 3): требования учитывают передовой опыт, стандарты, правила, классификации, зарекомендованное программное обеспечение и другие инструменты. Инструменты устанавливают последовательный подход к практике развертывания системы защиты. Гарантия проверяет реализацию на соответствие шаблонам безопасности.

– формализованный уровень (уровень 4): хорошо отлаженный процесс формирует основу для практической реализации, обеспечения постоянной поддержки и повышения безопасности. Гарантия реализации фокусируется на удовлетворении потребностей в безопасности и своевременном решении проблем, которые несут угрозу для системы.

Из вышеперечисленного следует, что большие числа указывают на более высокую степень полноты. Каждый уровень полноты покрывает все требования, установленные нижними уровнями, расширяя их.

В свою очередь, специфичность реализации практики можно оценить следующим образом:

– неспецифичный уровень (уровень 1): это самый широкий диапазон. Практика безопасности реализована без какой-либо оценки актуальности для конкретной отрасли и системы. Возможности и методы безопасности применяются так, как они были реализованы повсеместно.

– уровень специфичный для отросли (уровень 2): сфера применения сужена от общего случая к отраслевому сценарию. Практика безопасности реализуется с учетом отраслевых проблем, в частности, которые ка-

саются компонентов и процессов, которые подвержены определенным типам атак и известны уязвимости и произошедшие инциденты, присущие конкретной отрасли.

– уровень специфичный для системы (уровень 3): это самая узкая область. Реализация практики безопасности согласованы с конкретными организационными потребностями и рисками рассматриваемой системы, определены границы доверия, компоненты, технологии, процессы и сценарии использования.

В зависимости от контекста, возможно, что некоторые из практик могут оказаться неприменимыми. В этом случае они могут быть помечены как «Неприменима».

Для разработки модели зрелости безопасности АСУ ТП доменной печи необходимо оценить текущее состояние безопасности на объекте. Определение своей текущей зрелости безопасности и ее сравнение с целевым профилем дает возможность определить, что необходимо реализовать для перехода к более высокому состоянию зрелости, а также произвести адекватную оценку реализованных средств защиты и трезво оценить текущую ситуацию на объекте..

На рисунке 2 представлен текущий профиль безопасности АСУ ТП доменной печи ПАО «ММК» по полноте реализации практик.

Рассмотрим наиболее значимые практи-

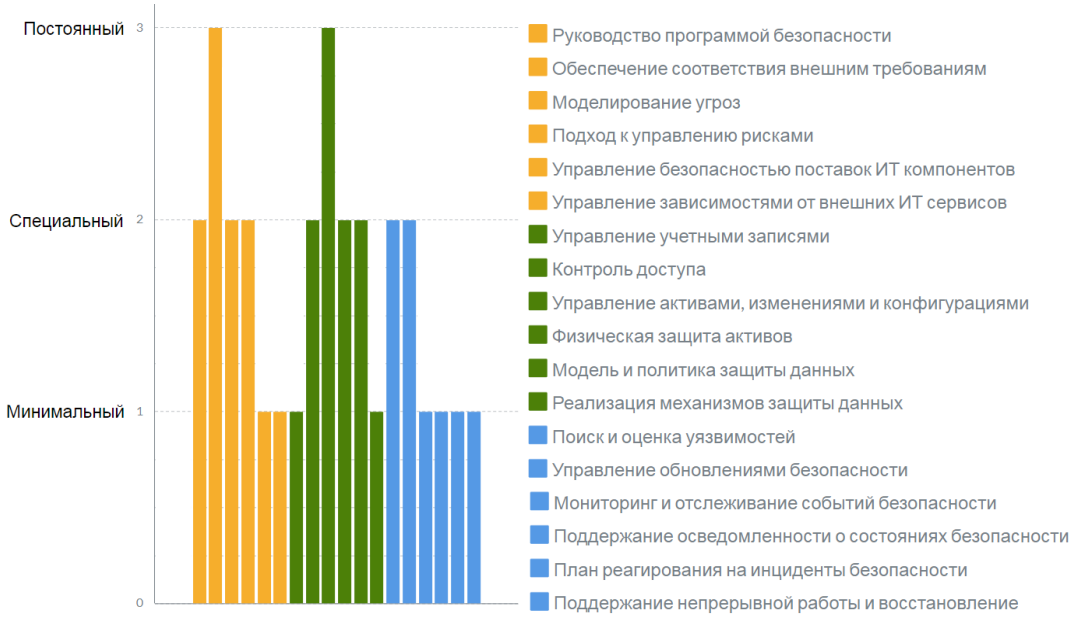

Рис. 2. Текущий профиль безопасности АСУ ТП доменной печи ПАО «ММК» по уровням полноты практик безопасности

ки для данной системы, которым был присвоен 3 уровень полноты.

1. Практика «Обеспечение соответствия внешним требованиям – постоянный уровень. Политика безопасности согласована со ФСТЭК России, объект категорирован и выполнены все требования законодательства в обеспечении безопасности на объекте критической информационной инфраструктуры.

2. Практика «Управление активами, изменениями и конфигурациями» - постоянный уровень. Классифицированы и маркированы физические и информационные активы, Политика управления изменениями включает в себя выявление значительных изменений в конфигурации системы и ПО. Разработаны руководящие принципы для защиты программного обеспечения, в том числе его целостности (внедрение антивирусных программ, реализация комплекса мероприятий по защите информации и обеспечению необходимым лицензионным ПО).

Модель зрелости помогает не только описать зрелость безопасности с разных точек зрения, в том числе с точки зрения бизнеса, но помогает согласовать и стимулировать сотрудничество среди всех заинтересованных сторон, которые работают над повышением зрелости безопасности. В то время как целевой профиль зрелости безопасности – это та цель предприятия, к которой необходимо стремиться для достижения зрелости безопасности с учетом текущих потребностей и производственных мощностей [5].

Составляя целевой профиль зрелости безопасности АСУ ТП, необходимо задавать следующие вопросы:

• Учитывая требования организации и ландшафт угроз, какова цель вашего решения?

• Каков текущий уровень зрелости безопасности на предприятии?

• Какие механизмы и процессы повлияют на переход текущего состояния безопасности в целевое состояние?

Уровень зрелости определяется с учетом полноты реализации практики безопасности и специфики ее реализации для АСУ ТП. Каждая организация, система, отдельное решение требует разной полноты и специфичности. Значит, и целевой уровень зрелости для разных случаев будет разным.

Переходы между уровнями определяются конкретными проблемами отрасли и системы, конкретными потребностями и рисками, выявленными при определении целевого уровня зрелости безопасности. Следовательно, перед оценкой зрелости безопасности заинтересованные стороны должны согласовать точные определения уровней полноты и охвата в соответствии с рисунком 3.

Из вышесказанного следует, что при уче-

Рис. 3. Состояния и переходы между уровнями полноты и специфичности реализации практик

те мощности бизнеса и потребности, не всегда присвоение 4 уровня как наилучшего будет рационально и осуществимо в ближайшей перспективе.

На рисунке 4 представлен целевой профиль безопасности АСУ ТП по полноте реализации практик.

Наиболее значимым практикам для данной системы был присвоен 4 уровень полноты. Это было сделано на основе следующих особенностей системы и приоритетов организации:

1. В силу того, что данный объект относится к критической информационной инфраструктуре (КИИ), необходимо постоянное совершенствование систем безопасности и соответствие нормативным документам по обеспечению безопасности КИИ. Поэтому целесообразно определить целевой уровень полноты практики «Обеспечение соответствия внешним требованиям» как формализованный.

2. Металлургическое производство зависит от непрерывной работы критически важных агрегатов, в работе оборудования могут возникать простои в связи с непредвиденными инцидентами информационной безопасности. Это влечет за собой большие экономические потери. Также следует отметить, что кибератака на АСУ ТП доменной печи может

Рис. 4. Целевой профиль зрелости безопасности по уровням полноты системы мониторинга состояния кожуха доменной печи ПАО «ММК»

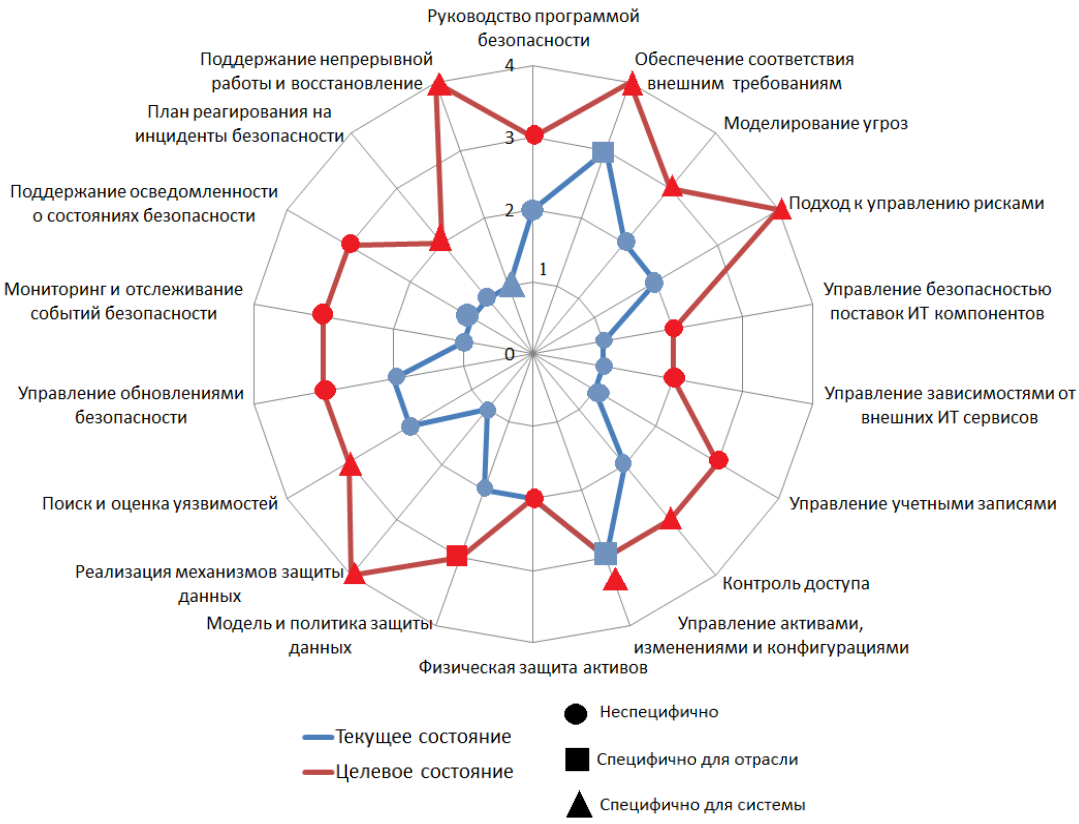

Рис. 5. Визуализация анализа расхождений текущего и целевого профиля зрелости безопасности при помощи паутинной диаграммы

привести к большим человеческим потерям, например, вследствие прорыва расплавленной шихты, а также повышает экологические риски. Согласно годовому отчету ММК [6] за 2020 год, в карте рисков ММК производственному и экологическому рискам присвоен высокий уровень. Поэтому для их снижения необходимо непрерывно управлять рисками и

разработать дорожную карту для их периодической переоценки. Поэтому следует практике «Управление рисками» присвоить 4 уровень полноты.

3. На основании вышесказанных пунктов для комплексной защиты информации выбранной системы необходимо реализовывать механизмы защиты на каждом этапе жизненного цикла системы, в том числе на этапе уничтожения. В связи с этим полнота практики «Реализация механизмов защиты» устанавливается на 4 уровне.

4. Обеспечение безотказной работы и непрерывности технологического процесса – самая приоритетная задача для производства [7]. Поэтому практика «Поддержание непрерывной работы и восстановление» должна стремиться к уровню 4.

Зная целевое состояние и текущее состояние, организация может выполнить анализ пробелов, чтобы определить подходящие области для улучшения безопасности и инвестиций. Для тех элементов управления, где есть разница между двумя состояниями, следует обратить внимание на размер разрыва, чтобы помочь при расстановке приоритетов в дорожной карте организации. Также необходимо обратить внимание на любые ситуации, в которых конкретный элемент управления может не соответствовать целевому состоянию, но потенциальный последующий риск смягчается другим средством контроля. Этот процесс должен дать список мер безопасности в организации, которые не соответствуют целевому состоянию.

На основе сравнения целевого и текущего состояния, заинтересованные стороны могут измерять прогресс и согласовывать шаги по повышению зрелости безопасности.

На рисунке 5 показана паутинной диаграмма, сравнивающая целевой и текущий профиль безопасности по полноте реализации практик. Маркеры на вершинах дают представление о специфичности реализации практик.

Пробелы в профилях определяются пробелами по полноте и специфичности. Если есть пробелы для конкретной (текущая зрелость практики ниже, чем хотелось бы), то эта практика должна быть улучшена. Если пробелов нет (одинаковые показатели уровня по практикам или текущее состояние выше целевого), то зрелость организации достаточна или опережает потребность.

Литература

1. Рудина, Е. Концепция nudge в обеспечении зрелости безопасности интернета вещей [Текст] / Е. Рудина // Технологическая перспектива в рамках Евразийского пространства: новые рынки и точки экономического роста: сб. науч. тр. – СПб.: Изд-во Центр научно-производственных технологий «Астерион», 2019. – Вып. 5 – С. 476-480.

2. Industrial Internet Consortium. IoT Security Maturity Model: Description and Intended Use Whitepaper. V1.1 of 2019-Feb-15. URL: https://iiconsortium.org/pdf/SMM Description and Intended Use FINAL Updated V1.1.pdf

3. Модель зрелости безопасности интернета вещей: толчок к развитию безопасных систем [Электронный ресурс] / Kaspersky ICS CERT - Электрон. дан. – М., 2019. – Режим доступа: https://ics-cert.kaspersky.ru/reports/2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity, свободный. — Загл. с экрана.

4. Федорова А.Р., Казаков О.А., Афанасьева М.В. Модель зрелости безопасности промышленного интернета вещей // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 79-й междун. науч.-технич. конф. 2021. С. 403.

5. Афанасьева М.В., Федосеев Н.А. Определение целевого профиля безопасности промышленного интернета вещей // Безопасность информационного пространства. Сборник трудов XIX Всерос. науч.-практич. конф. студентов, аспирантов и молодых ученых. Уральский государственный экономический университет. Екатеринбург, 2021. С. 197-200.

6. Годовой отчет ПАО «Магнитогорский металлургический комбинат» за 2019 год [Электронный ресурс] / Сайт группы ПАО «ММК» - Электрон. дан. – Магнитогорск, 2020. – Режим доступа: http://mmk.ru/for_investor/annual_reports/

7. Баранкова И.И., Михайлова У.В., Афанасьева М.В., Афанасьев М.Ю. Принципы построения модели надежности системы защиты информации АСУ ТП доменной печи // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 77-й междун. науч.-технич. конф. 2019. С. 424.

References

1. Rudina, Ye. Kontseptsiya nudge v obespechenii zrelosti bezopasnosti interneta veshchey [Tekst] / Ye. Rudina // Tekhnologicheskaya perspektiva v ramkakh Yevraziyskogo prostranstva: novyye rynki i tochki ekonomicheskogo rosta: sb. nauch. tr. – SPb.: Izd-vo Tsentr nauchno-proizvodstvennykh tekhnologiy "Asterion", 2019. – Vyp. 5 – S. 476-480.

2. Industrial Internet Consortium. IoT Security Maturity Model: Description and Intended Use Whitepaper. V1.1 of 2019-Feb-15. URL: https://iiconsortium.org/pdf/SMM Description and Intended Use FINAL Updated V1.1.pdf

3. Model' zrelosti bezopasnosti interneta veshchey: tolchok k razvitiyu bezopasnykh sistem [Elektronnyy resurs] / Kaspersky ICS CERT - Elektron. dan. – M., 2019. – Rezhim dostupa: https://ics-cert.kaspersky.ru/reports/2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity, svobodnyy. — Zagl. s ekrana.

4. Fedorova A.R., Kazakov O.A., Afanas'yeva M.V. Model' zrelosti bezopasnosti promyshlennogo interneta veshchey // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. Tezisy dokladov 79-y mezhdun. nauch.-tekhnich. konf. 2021. S. 403.

5. Afanas'yeva M.V., Fedoseyev N.A. Opredeleniye tselevogo profilya bezopasnosti promyshlennogo interneta veshchey // Bezopasnost' informatsionnogo prostranstva. Sbornik trudov XIX Vseros. nauch.-praktich. konf. studentov, aspirantov i molodykh uchenykh. Ural'skiy gosudarstvennyy ekonomicheskiy universitet. Yekaterinburg, 2021. S. 197-200.

6. Godovoy otchet PAO «Magnitogorskiy metallurgicheskiy kombinat» za 2019 god [Elektronnyy resurs] / Sayt gruppy PAO "MMK" - Elektron. dan. – Magnitogorsk, 2020. – Rezhim dostupa: http://mmk.ru/for_investor/annual_reports/

7. Barankova I.I., Mikhaylova U.V., Afanas'yeva M.V., Afanas'yev M.YU. Printsipy postroyeniya modeli nadezhnosti sistemy zashchity informatsii ASU TP domennoy pechi // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. Tezisy dokladov 77-y mezhdun. nauch.-tekhnich. konf. 2019. S. 424.

БАРАНКОВА Инна Ильинична, доктор технических наук, доцент, заведующая кафедрой информатики и информационной безопасности, Магнитогорский государственный технический университет им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Associate Professor, Head of the Department of computer science and information security, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: inna_barankova@mail.ru

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

AFANASYEVA Margarita Vladimirovna, Assistant Professor of the Department of computer science and information security, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: nansy_stokli@mail.ru

ФЕДОРОВА Анастасия Романовна, студент группы АИБ-19-2 кафедры информатики и информационной безопасности, Магнитогорский государственный технический университет им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: anastasia.43ag@gmail.com

FEDOROVA Anastasia Romanovna, student of the AIB-19-2 group of the Department of computer science and information security, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: anastasia.43ag@gmail.com