УДК 004.056.53 Вестник УрФО № 2(44) / 2022, с. 57–62

Баранкова И.И., Афанасьева М.В., Дегтярева А.В. DOI: 10.14529/secur220208

ПОСТРОЕНИЕ МОДЕЛИ ЗРЕЛОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ АСУ ТП ЦППН

В статье произведена адаптация методики построения модели зрелости безопасности интернета вещей под нужды и требования защиты объекта критической информационной инфраструктуры – цеха подготовки и перекачки нефти. В процессе работы былисмоделированы целевой и текущий профили.В статье приведены самые значимые практики по каждому из профилей, а также выведены диаграммы уровней полноты и специфики. Итогом работы стало приведенное в статье сравнение профилей с выявленными разрывами в обеспечении информационной защиты.

Ключевые слова: *информационная безопасность (ИБ), модель зрелости безопасности, критическая информационная инфраструктура (КИИ), автоматизированная система управления технологическим процессом (АСУ ТП), цех подготовки и перекачки нефти (ЦППН).*

Barankova I.I., Afanasyeva M.V., Degtyareva A.V.

BUILDING AN INFORMATION SECURITY MATURITY MODEL FOR THE APCS OF THE OIL TREATMENT AND PUMPING SHOP

The article adapts the methodology for building a security maturity model for the Internet of Things to the needs and requirements of protecting a critical information infrastructure object - an oil treatment and pumping shop. In the process of work, the target and current profiles were modeled. The article presents the most significant practices for each of the profiles, as well as diagrams of the levels of completeness and specificity. The result of the work was the comparison of profiles given in the article with the identification of gaps in information security.

Keywords: *information security (IS), security maturity model, critical information infrastructure (CII), automated process control system (APCS), oil treatment and pumping shop.*

На сегодняшний день прослеживается тенденция увеличения числа кибератак на организации всех типов, а нестабильная геополитическая ситуация обязывает еще пристальней обращать внимание на киберугрозы в критической инфраструктуре. Для того

чтобы выстроить адекватную программу информационной безопасности (ИБ), организации стали смотреть в сторону моделей зрелости. Модель зрелости призвана:

• Предоставлять организациям возможность эффективно оценивать и сравнивать показатели информационной безопасности.

• Определять пути развития и усовершенствования ИБ.

• Делиться знаниями и передовым опытом со смежными предприятиями, для усиления национальной безопасности.

Цель данной статьи – применить опыт построения модели зрелости для объекта КИИ – АСУ ТП ЦППН, который в дальнейшем поможет другим предприятиям выстроить или улучшить свою систему защиты ИБ.

Практически все современные модели зрелости основаны на модели CMM (CapabilityMaturityModel), разработанной и опубликованной в начале 1990-х гг. Институтом программной инженерии Карнеги – Мелона[1].

В 2019 году Kaspersky ICS CERT опубликовал руководство по применению модели IoTSecurityMaturityModel: Practitioner'sGuide. Эта модель направлена на интернет вещей, но в данной статье она была адаптирована под нужды и требования защиты КИИ (модель зрелости была разработана с учетом, что рассматриваемый объект имеет третью категорию значимости).

Модель зрелости ИБ строится путем сравнения целевого и текущего профилей безопасности. Целевой профиль зрелости представляет собой описание стопроцентной зрелости безопасности для системы, к достижению которой следует стремиться при ее развитии[2]. В текущем профиле зрелости безопасности определяется состояние защиты информации на предприятии в данный момент. Данные профили создаются путем определения набора пар «полнота+специфика» по всем практикам безопасности. Домены - это высокоуровневые представления, которые отражают ключевые аспекты зрелости безопасности: управление, внедрение и укрепление. Каждый из доменов имеет разные ключевые аспекты, называемые поддоменами. Например, домен усиления безопасности включает в себя поддомены уязвимости и обновления, ситуационная осведомленность и реагирование на события и инциденты. Далее каждый поддомен углубляется в две практики безопасности. Каждый домен может использовать различные методы, как технические, так и организационные, для достижения результатов в этой области. Такой иерархический подход позволяет рассматривать анализ зрелости на разных уровнях детализации - от различных областей в целом до отдельных практик [3].Иерархия доменов, поддоменов и практик в модели зрелости безопасности представлена в [4].

В рамках данной работы в первую очередь был смоделирован целевой профиль. Углубление осуществлялось до самого нижнего уровня – уровня практик. Следовательно, в работе были рассмотрены все восемнадцать практик, самые значимые приведены в статье.

В домене «Управление» особое внимание заслуживают практики «Руководство программой безопасности» и «Обеспечение соответствия внешним требованиям», так как они составляют базу защиты информации.

Для значимого объекта КИИ необходимо регулярно вести контроль, принимать стратегические решения относительно обеспечения безопасности, отслеживать технологические новинки, поэтому целевой уровень практики «Руководство программой безопасности» был определен как третий. Также данной практике был присвоен второй уровень специфики, так как внутренние документы, регулирующие вопросы, связанные с обеспечением ИБ, должны быть адаптированы под нужды и специфику производственного предприятия.

Всем значимым объектам КИИ предъявляются конкретные требования от регуляторов в зависимости от их категории значимости, в частности выполнение требований Приказа ФСТЭК России от 25 декабря 2017 г. N 239, следовательно, практика «Обеспечение соответствия внешним требованиям» имеет второй уровень, как у полноты, так и у специфики.

Далее были рассмотрены практики домена «Внедрение». Целевой уровень практики «Управление учетными записями» был определен как третий, так как согласно Приказу ФСТЭК №239 для данной системы необходимо организовать управление доступом с разделением полномочий пользователей, назначением минимально необходимых прав и привилегий и т.д. Используемое средство должно быть выбрано на основе анализа рынка передовых технологических решений. При этом специфике был присвоен первый уровень, так как процесс управления учетны-

ми записями может осуществляться через универсальные для любой другой типичной сферы программные продукты.

Для обеспечения защиты объекта должны быть отобраны лучшие, прошедшие сертификацию, средства защиты. Должен производиться мониторинг новинок. Это образует третий целевой уровень полноты практики «Реализация механизмов защиты данных». Необходимо учитывать совместимость средств защиты с системой, следовательно, специфика имеет третий уровень.

При инцидентах на значимом объекте КИИ необходимо: во первых, незамедлительно информировать о компьютерных инцидентах ФСБ России (НКЦКИ); во вторых, оказывать содействие должностным лицам ФСБ России в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов. Это образует второй целевой уровень полноты для практики «План реагирования на инциденты информационной безопасности» домена «Укрепление». Данные процессы будут иметь специфичный для индустрии характер, то есть второй уровень.

Для промышленного производства непрерывная работа является одним из ключевых приоритетов. В рамках практики «Поддержание непрерывной работы и восстановление» необходимо проводить организационные мероприятия по вопросам обеспечения НРВ, должны применяться различные способы резервирования аппаратных ресурсов, эталонного копирования программных и страхового копирования информационных ресурсов системы, а также проведение постоянного анализа эффективности принятых мер, разработка и реализация предложений по их совершенствованию[5]. Данные меры образуют третий целевой уровень полноты. Поддержание непрерывной работы должно учитывать особенности производственного процесса, следовательно, иметь второй уровень специфики.

Для наглядности получившийся целевой профиль был представлен графически (рисунок 1). Цветом выделены уровни специфики, а высота графиков отражает уровни полноты.

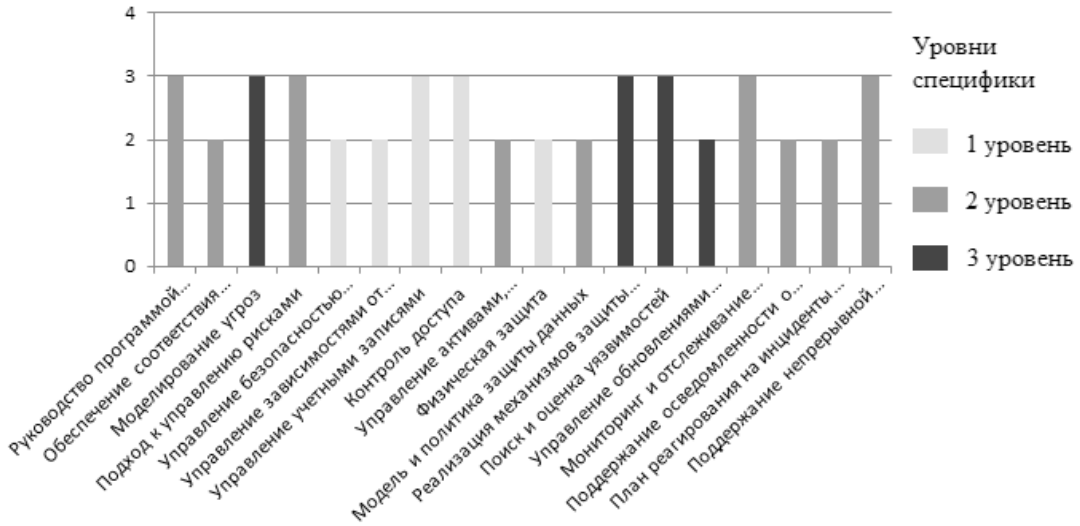

Рис. 1. Целевой профиль

На следующем этапе был смоделирован текущий профиль. Он создавался по тому же плану, что и целевой. Вначале были рассмотрены практики домена «Управление».В рамках данной работы было установлено, что практика «Руководство программой безопасности» на предприятии реализована на втором уровне полноты: руководством сформирован отдел по защите информации. В отделе выстроена иерархия, каждому сотруднику отведена зона ответственности (прописывание политик и контроль их соблюдения, настройка СЗИ и т.д.), начальник отдела контролирует все процессы, связанные с ИБ и отчитывается перед руководством. Все отмеченные процессы имеют специфичный для индустрии характер, то есть второй уровень.

На АСУ ТП ЦППН проведено категорирование объекта КИИ, результаты переданы во ФСТЭК, подготовлены все обязательные до-

кументы (модель угроз, политики) данные мероприятия определяют текущий уровень полноты и специфики как второй для практики «Обеспечение соответствия внешним требованиям».

Далее был рассмотрен домен «Внедрение». На предприятии реализуется управление учетными записями пользователей, в том числе внешних пользователей (возлагается на администратора ИБ): определение типа учетной записи; объединение учетных записей в группы; верификация пользователя; заведение, активация, блокирование и уничтожение учетных записей пользователей; пересмотр и, при необходимости, корректировка учетных записей не реже одного раза в три месяца; предоставление пользователям прав доступа к объектам доступа, основываясь на задачах, решаемых пользователями на предприятии. Все это образует второй текущий уровень полноты для практики «Управление учетными записями», при этом данные меры являются стандартными и применимы для любой типичной среды, поэтому присвоен первый уровень специфики.

На предприятии введены в действие сертифицированные ФСТЭК программные и технические продукты по защите информации, но их недостаточно для покрытия всех актуальных угроз, также есть средства с истекшими сертификатами.На основе этих данных, практике «Реализация механизмов защиты данных» был присвоен первый текущий уровень полноты. При подборе средств, специалисты учитывалисовместимость средств защиты с системой, следовательно, специфика имеет третий уровень.

На последнем этапе рассматривался домен «Укрепление». Практика «План реагирования на инциденты информационной безопасности» реализован на втором уровне полноты, так как план реагирования задокументирован, при возникновении инцидентов обеспечивается незамедлительное информирование ФСБ России (НКЦКИ); оказывается содействие должностным лицам ФСБ России в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов. Данные процессы имеют специфичный для индустрии характер, то есть второй уровень.

На АСУ ТП ЦППН проводятся организационные мероприятия по вопросам обеспечения НРВ, применяется система горячего резервирования SCADA TRACE MODE. Данные меры образуют второй текущий уровень полноты для практики «Поддержание непрерывной работы и восстановление». Поддержание непрерывной работы учитывает особенности производственного процесса, следовательно, имеет второй уровень специфики.

Для наглядности получившийся текущий профиль был представлен графически (рисунок 2).

Завершающим этапом работы стало построение графика сравнения двух профилей (рисунок 3), это и есть модель зрелости.

Из построенной модели зрелости видно,

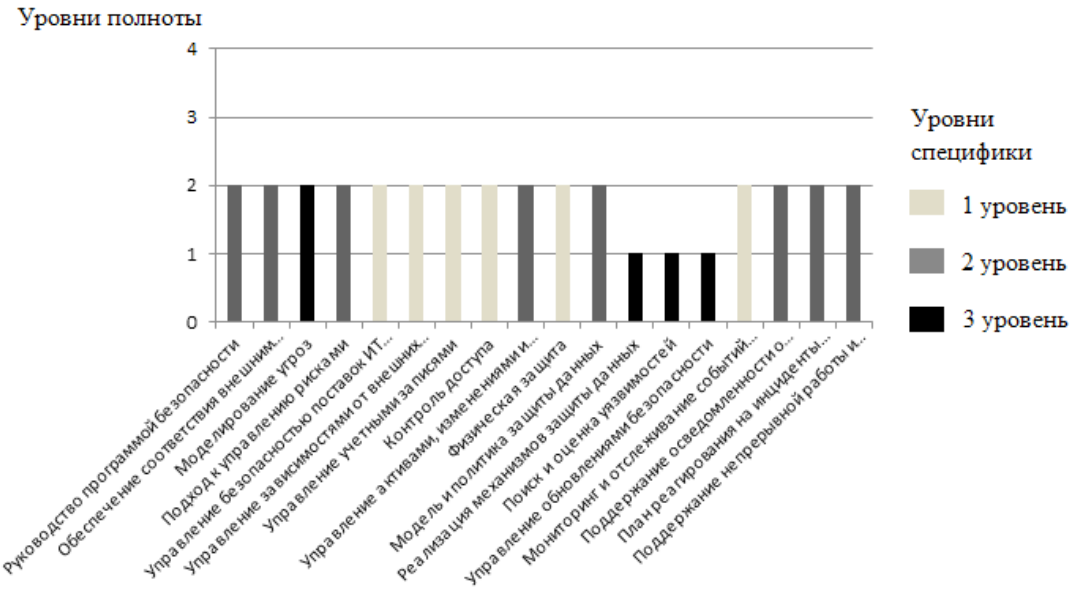

Рис. 2. Текущий профиль

Рис. 3. Модель зрелости

что критические разрывы имеют практики «Реализация механизмов защиты данных» и «Поиск и оценка уязвимостей», что свидетельствует о необходимости принятия кардинальных мер по модернизации данных направлений. Остальные восемнадцать практик разделились поровну: либо текущий уровень соответствует целевому, и от предприятия требуется лишь поддерживать защиту в ее текущем состоянии, либо имеется разрыв в один уровень и предприятию необходимо увеличить степень защиты в данном направлении. Если грамотно воспользоваться данной моделью, то она может стать эффективным инструментом в создании качественной системы защиты.

На основе модели зрелости любая компания может увидеть пробелы в своей системе защиты и эффективно закрыть подавляющее число уязвимостей. Данная работа может стать базой для проведения работ в сфере обеспечения информационной защиты на промышленных предприятиях, а также может быть легко адаптированадля обеспечения корпоративной защиты.

Литература

1. Борисов И.С. Обзор уровня зрелости процессов ИБ: о трендах и методологиях. Information Seecurity, 2019. – Режимдоступа: https://www.itsec.ru/articles/obzor-urovnya-zrelosti-protsessov-ib-o-trendakh-i-metodologiyakh.

2. Рудина Е.А., Гончаров Е.В. Модель зрелости безопасности интернета вещей: толчок к развитию безопасных систем. Kaspersky ICS CERT, 2019. – Режим доступа: https://ics-cert.kaspersky.ru/reports/2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity/.

3. Рудина Е.А. Модель зрелости и безопасности IoT. Connect-WIT, 2019. – Режим доступа: https://www.connect-wit.ru/model-zrelosti-i-bezopasnosti-iot.html.

4. Баранкова И.И., Афанасьева М.В., Федорова А.Р. Модель зрелости безопасности АСУ ТП доменной печи №10 ПАО «ММК». Актуальные проблемы кибербезопасности, Вестник УрФО № 3(41), 2021, с. 57–64.

5. 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. Borisov I.S. Obzor urovnja zrelosti processov IB: o trendah i metodologijah. Information Seecurity, 2019. – Rezhimdostupa: https://www.itsec.ru/articles/obzor-urovnya-zrelosti-protsessov-ib-o-trendakh-i-metodologiyakh.

2. Rudina E.A., Goncharov E.V. Model' zrelosti bezopasnosti interneta veshhej: tolchok k razvitiju

bezopasnyh sistem. Kaspersky ICS CERT, 2019. – Rezhim dostupa: https://ics-cert.kaspersky.ru/reports/2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity/.

3. Rudina E.A. Model' zrelosti i bezopasnosti IoT. Connect-WIT, 2019. – Rezhim dostupa: https://www.connect-wit.ru/model-zrelosti-i-bezopasnosti-iot.html.

4. Barankova I.I., Afanas'eva M.V., Fedorova A.R. Model' zrelosti bezopasnosti ASU TP domennoj pechi №10 PAO «MMK». Aktual'nye problemy kiberbezopasnosti, Vestnik UrFO № 3(41), 2021, s. 57–64.

5. Barankova I.I., Mihajlova U.V., Afanas'eva M.V., Afanas'ev M.Ju. Principy postroenija modeli nadezhnosti sistemy zashhity informacii ASU TP domennoj pechi. Aktual'nye problemy sovremennoj nauki, tehniki i obrazovanija. Tezisy dokladov 77-j Mezhdun. Nauch.-Tehnich. 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

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

ДЕГТЯРЕВА Алена Владимировна, студент кафедры информатики и информационной безопасности, Магнитогорский государственный технический университет им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: alenastudy5@yandex.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, LeninAve., 38. E-mail: inna_barankova@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

DEGTYAREVA Alena Vladimirovna, student of the Department of computer science and information security, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: alenastudy5@yandex.ru