DOI: 10.55648/1998-6920-2024-18-2-88-102 УДК 004.056

Оценка уровня доверия к процессу управления инцидентами информационной безопасности

А. В. Иванов, И. А. Огнев, И. В. Никрошкин, М. А. Киселев

Новосибирский государственный технический университет (НГТУ)

Аннотация: Существующие методики оценки уровня доверия к процессу управления инцидентами информационной безопасности и к процессам систем мониторинга событий информационной безопасности крайне ограничены. Данные методики основаны на экспертной оценке и носят периодический характер с большим промежутком времени между оценками. Целью данного исследования является разработка методики оценки уровня доверия к процессу управления инцидентами информационной безопасности, которая позволит проводить оценку в автоматизированном режиме с минимальным участием экспертов. В результате была разработана методика оценки уровня доверия к процессу управления инцидентами информационной безопасности, которая включает в себя перечень критериев доверия и метрик для их оценки, в её основе лежит методика SOMM и ГОСТ ISO/IEC 27035. Разработанная методика основана на трехэтапной оценке показателей доверия: оценка метрик доверия, оценка критериев доверия, оценка уровня доверия к процессу управления инцидентами информационной безопасности. Сформирован математический аппарат расчета числовых значений метрик доверия, критериев доверия и общего уровня доверия к процессу управления инцидентами информационной безопасности. Разработанная методика может быть включена в общую методику оценки уровня доверия к процессам информационной безопасности, входящим в состав процесса мониторинга событий информационной безопасности.

Ключевые слова: инциденты информационной безопасности, управление инцидентами, оценка процессов, уровень доверия, доверие, информационная безопасность, мониторинг информационной безопасности, кибербезопасность.

Для цитирования: Иванов А. В., Огнев И. А., Никрошкин И. В., Киселев М. А. Оценка уровня доверия к процессу управления инцидентами информационной безопасности // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 88–102. https://doi.org/10.55648/1998-6920-2024-18-2-88-102.

Статья поступила в редакцию 09.02.2024;
принята к публикации 29.02.2024.

1. Введение

Переход к более высокому уровню развития компании осуществляется путем улучшения ее показателей при положительной динамике ключевых характеристик [1–6]. Это делает организацию более конкурентоспособной, позволяет динамично реагировать на требования рынка и оптимально использовать свои внутренние ресурсы. Существуют определенные подходы к оценке каждого уровня развития компании: например, модели, описывающие этапы развития, известные как модели уровней зрелости.

В области информационной безопасности (ИБ) использование моделей зрелости может помочь выделить организации, в которых информационная безопасность полностью интегрирована в бизнес-процессы, из тех, где она выполняет в основном вспомогательную функцию: соответствие стандартам для закрытия основных требований ИБ [7–10]. Это, в свою очередь, демонстрирует уровень доверия к организации с точки зрения контрагентов. Поэтому в данном исследовании оценку уровня доверия к процессу управления инцидентами информационной безопасности будем приравнивать к оценке уровня зрелости процесса управления инцидентами информационной безопасности.

Одна из ключевых причин использования моделей зрелости в данном контексте заключается в том, что внедрение улучшений по всей организации требует значительного времени. В области кибербезопасности модель зрелости предоставляет руководству средство оценки прогресса в обеспечении безопасности в повседневных и стратегических задачах. Эта модель служит инструментом для оценки эффективности интеграции бизнес-процессов в организации, позволяя руководству установить долгосрочные цели и эффективно отслеживать прогресс. Применение моделей зрелости также помогает компаниям выявлять свои сильные и слабые стороны.

Подобно моделям зрелости, где компании оценивают свой уровень зрелости в определенных областях, оценка доверия [11] к управлению инцидентами позволяет определить, насколько организация доверяет своим контрагентам в вопросах управления инцидентами информационной безопасности и в сфере информационной безопасности в целом. Этот подход помогает выявить сильные стороны, а также слабые места в управлении инцидентами, что, в свою очередь, способствует разработке и реализации улучшений для повышения эффективности и надежности процесса управления инцидентами информационной безопасности.

2. Постановка задачи исследования

Существующее количество методик для оценки зрелости процессов управления инцидентами в области информационной безопасности крайне ограничено [12–17], и все они являются зарубежными. Одной из самых популярных методик, позволяющих в той или иной степени оценить качество процесса управления инцидентами информационной безопасности, является методика SOMM (Security Operations Maturity Model) [12], разработанная Университетом Карнеги–Меллона (Carnegie Mellon University). Данная методика включает в себя 5 ключевых уровней зрелости от 0 до 5, уровни зрелости данной методики представлены в табл. 1. Оценка управления инцидентами информационной безопасности разбивается на поддиапазоны от недостаточного до экстремального уровня оценки зрелости. Но у данной методики есть несколько недостатков, которые не позволяют полноценно оценить зрелость процесса управления инцидентами информационной безопасности на всех его этапах. Описание каждого уровня не включает в себя набор определенных метрик, позволяющий более точно и правильно оценить ключевые процессы управления инцидентами информационной безопасности. Вторым недостатком данной методики является экспертная оценка, которая больше зависит от человеческого фактора и не представляет возможности объективно оценить процессы управления инцидентами информационной безопасности.

Для решения данной проблемы была продумана и разработана собственная методика оценки уровня доверия (зрелости) к процессам управления инцидентами информационной безопасности, включающая в себя 6 основных критериев и более 30 метрик для проведения качественной и объективной оценки выполнения процессов управления инцидентами информационной безопасности. Выбор 6 основных критериев для методики оценки зрелости процессов управления инцидентами информационной безопасности обоснован стремлением охватить важнейшие аспекты и этапы данного процесса. Каждый из этих критериев представляет ключевой этап в жизненном цикле управления инцидентами, обеспечивая комплексное понимание и оценку эффективности системы безопасности организации. Выбор 34 метрик для

оценки зрелости процессов управления инцидентами информационной безопасности обусловлен необходимостью получения детального и многогранного представления об эффективности каждого из выбранных критериев. Каждая метрика была тщательно отобрана для того, чтобы внести специализированный вклад в измерение конкретных аспектов каждого этапа управления инцидентами. Критерии и метрики процесса управления инцидентами информационной безопасности представлены на рис 1.

Таблица 1. Уровни зрелости по методике SOMM

Уровень SOMM	**Оценка управления инцидентами ИБ**	**Описание**
Уровень 0	Недостаточный	Ключевые составляющие управления инцидентами ИБ (мониторинг, документирование, SLA) отсутствуют.
Уровень 1	Начальный	Управление инцидентами присутствует, но нет документированных процессов.
Уровень 2	Базовый	Выполнение нормативных и бизнес-требований. Большинство процессов управления документированы, но пересматриваются по ситуации.
Уровень 3	Надлежащий	Процессы управления хорошо документированы, регулярно пересматриваются с учетом текущих лучших практик.
Уровень 4	Осмысленный	Эффективность управления инцидентами регулярно оценивается по метрикам производительности. Процессы выстраиваются для достижения KPI бизнеса.
Уровень 5	Экстремальный	По всем направлениям управления инцидентами приняты программы развития. Процессы максимально конкретизированы и отточены.

3. Методика оценки доверия к процессу управления инцидентами информационной безопасности

Предлагаемая методика реализации процесса оценки уровня доверия к процессу управления инцидентами информационной безопасности включает в себя трехэтапную иерархическую оценку показателей доверия:

1. Оценка метрик доверия.
2. Оценка критериев доверия – подпроцессы процесса управления инцидентами информационной безопасности.
3. Оценка уровня доверия к процессу управления инцидентами информационной безопасности.

В качестве критериев будем использовать следующие подпроцессы [18]:

1. Планирование и подготовка.
2. Обнаружение и оповещение.
3. Оценка и принятие решений.
4. Расследование инцидентов ИБ.
5. Реагирование на инциденты ИБ.
6. Улучшение процесса управления инцидентами ИБ.

Каждый из критериев оценивается по определенной шкале, и на основе совокупности оценок формируется общая картина доверия к процессу управления инцидентами ИБ.

Каждый из этих критериев сопровождается набором конкретных метрик, которые также подвергаются оценке. Этот процесс позволяет получить конечные объективные результаты для каждой метрики и каждого критерия. Таким образом формируется итоговая оценка

доверия к процессу управления инцидентами ИБ на основе совокупности оценок, обеспечивая глубокое понимание эффективности данных процессов в организации.

Опишем кратко все этапы процесса управления инцидентами информационной безопасности для формирования эффективной оценки доверия.

3.1. Планирование и подготовка

Первый этап является началом построения процесса управления инцидентами ИБ и включает в себя формирование основных регламентов и актов, позволяющих в дальнейшим использовать их для построения грамотного процесса управления инцидентами ИБ. В данный подпроцесс входят создание политики управления инцидентами ИБ, создание группы по реагированию на инциденты ИБ, формирование внутреннего и внешнего SLA организаций и др.

3.2. Обнаружение и оповещение

Второй этап управления инцидентами ИБ – обнаружение и оповещение – в рамках управления инцидентами информационной безопасности включает в себя выявление событий ИБ, сбор и обобщение связанной с ними информации, а также создание отчетов о их возникновении и выявленных уязвимостях с применением как ручных, так и автоматических методов.

3.3. Оценка и принятие решений

На данном этапе формируется оценка степени серьезности события/инцидента ИБ после факта его выявления системой мониторинга или каким-либо другим средством экспертизы анализа данных. Также на данном этапе производится актуализация баз данных ИБ для формирования правильной и точной оценки события ИБ.

3.4. Расследование инцидентов ИБ

Четвертый этап является одним из ключевых подпроцессов управления инцидентами ИБ и включает в себя формирование регламента по расследованию инцидентов ИБ, в котором отражаются следующие ключевые шаги:

- распределение обязанностей и ответственности среди специалистов для эффективного проведения расследования;
- формирование версий, объясняющих причины возникновения инцидента;
- приоритизация версий по степени вероятности возникновения инцидента ИБ на основе сформированной базы знаний с этапа «Оценка и принятие решений», а также на базе собственного опыта.

Заканчивается данный этап на создании отчета о проведении расследования и передачи информации группе реагирования на инциденты ИБ.

3.5. Реагирование на инциденты ИБ

Пятый этап управления инцидентами информационной безопасности – реагирование на инциденты ИБ – нацелен на эффективное устранение последствий инцидента и восстановление штатного функционирования информационной системы организации. Данный этап также является ключевым подпроцессом управления инцидентами информационной безопасности. Четвертый и пятый этапы, по сути, являются основными этапами всего процесса управления инцидентами. Исходя из имеющихся данных, эти два этапа являются неразрывными друг для друга, поэтому продуманный и тщательно проанализированный этап расследования приведет к качественным мерам реагирования на инциденты ИБ.

Рис. 1. Зрелость процесса управления инцидентами информационной безопасности

3.6. Улучшение процесса управления инцидентами ИБ

Шестой этап является заключительным в формировании процесса управления инцидентами ИБ. На данном этапе формируются результаты расследования и реагирования на инциденты. С целью усовершенствования процесса управления инцидентами анализируются все

предыдущие шаги и выявляются слабые стороны одного из перечисленных ранее процессов для их дальнейшего усовершенствования.

Итоговый набор всех критериев оценки доверия к процессам управления инцидентами ИБ и их метрикам представлен на рис. 1.

4. Показатели оценки уровня доверия

4.1. Формирование математического аппарата

За основу методики расчета уровня доверия возьмем процедуру оценки соответствия – ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. Методика оценки соответствия» [19].

Настоящий стандарт содержит в себе требования к методике и оформлению результатов проведенной проверки в соответствии с ГОСТ Р 57580.1-2017 [20] и предназначен для организаций, осуществляющих оценку соответствия защиты информации (ЗИ) финансовых организаций.

ГОСТ Р 57580.1-2017 определяет пять уровней соответствия ЗИ (табл. 2).

Таблица 2. Уровни соответствия ЗИ по ГОСТ Р 57580.1-2017

Уровень соответствия	**Реализация мер ЗИ**	**Подход к реализации мер ЗИ**	**Контроль и совершенствование системы ЗИ**
Нулевой	Не реализуются / реализуются бессистемно	Нет общего подхода	Отсутствует
Первый	Реализуются бессистемно в незначительном количестве	Нет общего подхода	Отсутствует
Второй	Реализуются в полном / практически полном объеме на постоянной основе	Общие подходы установлены в единичных случаях	Практически отсутствует
Третий	Реализуются в полном / практически полном объеме на постоянной основе	Общие подходы установлены в значительном количестве	Бессистемный / эпизодический контроль и совершенствование
Четвертый	Реализуются в полном / практически полном объеме на постоянной основе	Общие подходы установлены в значительном количестве	Системный контроль и совершенствование
Пятый	Реализуются в полном / практически полном объеме на постоянной основе	Общие подходы установлены в значительном количестве	Постоянный контроль и совершенствование

Для каждого раздела мер стандарт устанавливает свою систему оценок соответствия, например, Раздел 8. «Требования к организации и правлению защитой информации». Для оценок, характеризующих полноту реализации каждой из мер, определяют следующие числовые значения:

- 0 – мера не реализуется, т.е. у проверяющей организации отсутствуют свидетельства реализации оцениваемой меры;
- 0.5 – мера реализуется частично, не в полном объеме;
- 1 – мера реализуется в полном объеме, т.е. проверяющей организации предоставлены свидетельства полной реализации оцениваемой меры.

В данном ГОСТ также перечисляются основные источники свидетельств, на основании которых выставляются оценки соответствия:

• документы и иные материалы проверяемой организации в бумажном или электронном виде и при необходимости документы третьих лиц, относящиеся к обеспечению ЗИ финансовой организации и находящиеся в распоряжении проверяемой организации;

• устные высказывания сотрудников проверяемой организации в процессе проводимых опросов в области оценки соответствия ЗИ;

• результаты наблюдений членов проверяющей группы за процессами системы ЗИ и деятельностью сотрудников проверяемой организации в области оценки соответствия ЗИ;

• параметры конфигураций и настроек технических объектов информатизации и средств ЗИ;

• технические и программные средства сбора свидетельств полноты реализации мер ЗИ (анализ электронных журналов регистрации, анализ фактических настроек, анализ уязвимостей, проведение тестирования на проникновение и т.п.).

В завершении методики оценивания есть качественная и количественная оценка соответствия процессов ЗИ. Качественная оценка выставляется в соответствии с приведенной в стандарте таблицей, которая, в свою очередь, основывается на расчетных значениях. Ниже приведена табл. 3 для качественной оценки уровня соответствия.

Таблица 3. Качественная оценка соответствия процессов системы ЗИ

E_i	**Уровень соответствия**
$E_i = 0$	Нулевой
$0 < E_i \leq 0.5$	Первый
$0.5 < E_i \leq 0.7$	Второй
$0.7 < E_i \leq 0.85$	Третий
$0.85 < E_i \leq 0.9$	Четвертый
$0.9 < E_i \leq 1$	Пятый

E_i – сумма числовых оценок контуров безопасности с учетом их весовых коэффициентов. Количественную оценку вычисляют как среднеарифметическое значение оценок E_i для всех процессов системы защиты информации и оценки полноты применения организационных и технических мер на этапах жизненного цикла без учета количества нарушений, выявленных проверяющей группой в процессе аудита.

4.2. Расчет показателей доверия

Взяв за основу ГОСТ Р 57580.1-2017, формализуем формулы для расчета каждого этапа оценки уровня доверия к процессу управления инцидентами информационной безопасности:

Показатели 1 этапа – метрики оценки уровня доверия к процессу управления инцидентами ИБ:

$$E_{1\text{ji}} = \begin{cases} 0, & \text{доказательство доверия отсутствует} \\ 1, & \text{доказательство доверия присутствует} \end{cases}, \quad (1)$$

где E_{1ji} – i-й показатель 1-го этапа (метрика) для вычисления j-го показателя 2-го этапа (критерия).

Показатели 2-го этапа – критерии оценки уровня доверия к процессу управления инцидентами ИБ:

$$E_{2j} = \frac{\sum_{i=1}^{N_j} E_{1ji}}{N_j}, \quad (2)$$

где E_{2j} – j-й показатель 2-го этапа (критерий), E_{1ji} – i-й показатель 1-го этапа (метрика) для вычисления j-го показателя 2-го этапа (критерия), N_j – количество показателей 1-го этапа (метрик), предназначенных для вычисления j-го показателя 2-го этапа (критерия).

Показатели 3-го этапа – уровень доверия к процессу управления инцидентами ИБ:

$$E = \frac{\sum_{j=1}^{N} E_{2j}}{N}, \quad (3)$$

где E – уровень доверия (зрелости) к процессу управления инцидентами информационной безопасности, E_{2j} – j-й показатель 2-го этапа (критерий), N – количество показателей 2-го этапа (критериев), предназначенных для вычисления показателя 3-го этапа (уровня доверия). В нашем случае $N = 6$.

При этом в качестве доказательств доверия (источников информации для оценки уровня доверия) будем использовать автоматизированный анализ составляющих организационно-правового поля исследуемой организации.

Соответствие уровней доверия к процессу управления инцидентами информационной безопасности основано на уровнях соответствия ГОСТ Р 57580.1-2017 (табл. 3).

4.3. Метрики доверия

Далее рассмотрим метрики оценки каждого критерия доверия, которые были определены выше:

1. Планирование и подготовка.
2. Обнаружение и оповещение.
3. Оценка и принятие решений.
4. Расследование инцидентов ИБ.
5. Реагирование на инциденты ИБ.
6. Улучшение процесса управления инцидентами ИБ.

4.3.1. Метрики оценки доверия к критерию «Планирование и подготовка»

Пусть критерий «Планирование и подготовка» будет иметь обозначение E_{21}, тогда метрики оценки данного критерия будут носить обозначения E_{11i} (табл. 4).

Таблица 4. Метрики оценки доверия к критерию «Планирование и подготовка»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{111}	Наличие политики управления инцидентами ИБ	[0, 1]
E_{112}	Наличие регламента по обновлению политики управления инцидентами ИБ	[0, 1]
E_{113}	Наличие плана управления инцидентами ИБ	[0, 1]
E_{114}	Наличие приказа о формировании группы реагирования на инциденты ИБ	[0, 1]
E_{115}	Наличие регламента взаимодействия с внутренними и внешними организациями по вопросам управления инцидентами ИБ	[0, 1]
E_{116}	Наличие регламента по повышению квалификации специалистов по управлению инцидентами ИБ	[0, 1]
E_{117}	Наличие журнала прохождения повышения квалификации специалистами по управлению инцидентами ИБ	[0, 1]

E_{118}	Наличие акта, подтверждающего факт проведения киберучений	[0, 1]
E_{119}	Наличие внутреннего и внешнего SLA	[0, 1]

Тогда количество метрик в данном критерии $N_1 = 9$.

4.3.2. Метрики оценки доверия к критерию «Обнаружение и оповещение»

Пусть критерий «Обнаружение и оповещение» будет иметь обозначение E_{22}, тогда метрики оценки данного критерия будут носить обозначения E_{12i} (табл. 5).

Таблица 5. Метрики оценки доверия к критерию «Обнаружение и оповещение»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{121}	Наличие регламента по осуществлению мониторинга ИС	[0, 1]
E_{122}	Наличие регламента по журналированию событий ИБ в ИС	[0, 1]
E_{123}	Наличие регламента по анализу сетевой активности в ИС	[0, 1]
E_{124}	Наличие регламента по подключение источников к системе мониторинга ИБ организации	[0, 1]
E_{125}	Наличие регламента по инвентаризации активов ИС	[0, 1]
E_{126}	Наличие регламента оповещения о событии/уязвимости ИБ	[0, 1]
E_{127}	Наличие отчетов о реагировании на КИ	[0, 1]

Тогда количество метрик в данном критерии $N_2 = 7$.

4.3.3. Метрики оценки доверия к критерию «Оценка и принятие решений»

Пусть критерий «Оценка и принятие решений» будет иметь обозначение E_{23}, тогда метрики оценки данного критерия будут носить обозначения E_{13i} (табл. 6).

Таблица 6. Метрики оценки доверия к критерию «Оценка и принятие решений»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{131}	Наличие регламента по формированию степени серьезности события ИБ	[0, 1]
E_{132}	Наличие регламента о передаче события/инцидента в группу по расследованию инцидентов ИБ	[0, 1]
E_{133}	Наличие регламента контроля за изменениями и обновлениями баз знаний ИБ	[0, 1]
E_{134}	Наличие журнала обновлений изменений баз знаний ИБ	[0, 1]

Тогда количество метрик в данном критерии $N_3 = 4$.

4.3.4. Метрики оценки доверия к критерию «Расследование инцидентов ИБ»

Пусть критерий «Расследование инцидентов ИБ» будет иметь обозначение E_{24}, тогда метрики оценки данного критерия будут носить обозначения E_{14i} (табл. 7).

Таблица 7. Метрики оценки доверия к критерию «Расследование инцидентов ИБ»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{141}	Наличие регламента по расследованию инцидентов информационной безопасности	[0, 1]
E_{142}	Наличие акта о внедрении средств автоматизации процесса обогащения данных об инциденте ИБ	[0, 1]
E_{143}	Наличие отчета о проведении расследования инцидента ИБ	[0, 1]
E_{144}	Наличие формы отчета о проведении расследования инцидента ИБ	[0, 1]

Тогда количество метрик в данном критерии $N_4 = 4$.

4.3.5. Метрики оценки доверия к критерию «Реагирование на инциденты ИБ»

Пусть критерий «Реагирование на инциденты ИБ» будет иметь обозначение E_{25}, тогда метрики оценки данного критерия будут носить обозначения E_{15i} (табл. 8).

Таблица 8. Метрики оценки доверия к критерию «Реагирование на инциденты ИБ»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{151}	Наличие регламента по реагированию на инциденты информационной безопасности	[0, 1]
E_{152}	Наличие отчета о проведении мероприятий по реагированию на инцидент ИБ	[0, 1]
E_{153}	Наличие формы отчета о проведении мероприятий по реагированию на инцидент ИБ	[0, 1]
E_{154}	Наличие инструкции об использовании средств автоматизации процесса обогащения данных об инциденте ИБ	[0, 1]
E_{155}	Наличие информации об инцидентах ИБ в перечне конфиденциальной информации организации	[0, 1]

Тогда количество метрик в данном критерии $N_5 = 5$.

4.3.6. Метрики оценки доверия к критерию «Улучшение процесса управления инцидентами информационной безопасности»

Пусть критерий «Улучшение процесса управления инцидентами информационной безопасности» будет иметь обозначение E_{26}, тогда метрики оценки данного критерия будут носить обозначения E_{16i} (табл. 9).

Таблица 9. Метрики оценки доверия к критерию
«Улучшение процесса управления инцидентами информационной безопасности»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{161}	Наличие регламента обработки результатов расследования и реагирования на инциденты ИБ	[0, 1]
E_{162}	Наличие журнала изменений системы защиты информации	[0, 1]
E_{163}	Наличие регламента по проведению киберучений	[0, 1]
E_{164}	Наличие KPI для сотрудников группы по расследованию инцидентов ИБ	[0, 1]
E_{165}	Наличие KPI для сотрудников группы по реагированию на инциденты ИБ	[0, 1]

Тогда количество метрик в данном критерии $N_6 = 5$.

5. Заключение

Разработана методика оценки уровня доверия (зрелости) к процессу управления инцидентами информационной безопасности, позволяющая провести автоматизированную оценку на основе объективных показателей, снижая при этом влияние человеческого фактора и повышая скорость её проведения за счет возможности применения средств автоматизации. Методика основана на анализе нормативно-правовых аспектов центров мониторинга за состоянием безопасности информационных систем (SOC). Сформированная методика содержит в себе набор критериев и метрик доверия для проведения оценки, набор формул для расчета каждой метрики и критериев доверия, а также формулу расчета итогового уровня доверия к процессу управления инцидентами информационной безопасности.

Разработанная методика может быть доработана путём анализа технических аспектов SOC и всей организации в целом. Помимо этого, данная методика может войти в состав общей методики оценки уровня доверия к процессам SOC, которая будет направлена на комплексный анализ всех процессов мониторинга безопасности информационных систем с целью получения объективных свидетельств, позволяющих в автоматизированном режиме провести расчет уровня зрелости SOC.

Литература

1. *Велигодский С. С., Милославская Н. Г.* Унифицированная модель зрелости центров управления сетевой безопасностью информационно-телекоммуникационных сетей // Известия ЮФУ. Технические науки. 2023. №3 (233). С. 157–172.
2. *Селезнёв В. М., Боровская О. Е.* Встраивание инструментов SOAR-платформ в экосистему SOC для автоматизации процесса реагирования на инциденты ИБ // Международный научно-исследовательский журнал. 2022. № 10 (124). С. 1–9.
3. *Веревкин С. А., Кравчук А. В., Беляков М. И.* Методика управления инцидентами информационной безопасности на объектах критической информационной инфраструктуры // Известия Тульского гос. университета. Технические науки. 2022. № 8. С. 116–120.
4. *Сухов А. М.* Оценивание эффективности процесса функционирования системы обеспечения информационной безопасности на основе теории стохастической индикации // Информационно-управляющие системы. 2022. № 3. С. 31–44.
5. *Иванов А. В., Никрошкин И. В. , Огнев И. А., Киселев М. А.* Применение средств экспертизы Blue Team в процессе мониторинга информационных систем на примере платформы TI

(Threat Intelligence) // Безопасность цифровых технологий. 2023. № 2 (109). С. 34–51. DOI: 10.17212/2782-2230-2023-2-34-51.
6. *Рева И. Л., Медведев М. А., Воронцова И. В.* Исследование проблематики методик определения типа контента во входящем трафике // Системы анализа и обработки данных. 2022. № 4 (92). С. 69–84. DOI: 10.17212/2782-2001-2023-4-69-84.
7. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
8. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
9. Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
10. Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
11. *Селифанов В. В., Аникеева В. В., Огнев И. А.* Вопросы оценки доверия к системе управления рисками // Безопасность цифровых технологий. 2023. № 1 (108). С. 69–82. DOI: 10.17212/2782-2230-2023-1-69-82.
12. Security Operations Maturity Model // StarLink. [Электронный ресурс] Режим доступа: https://assets.starlinkme.net/gitex-vendor-assets/logrhythm/uk-security-operations-maturity-model-white-paper.pdf (дата обращения: 30.01.2024).
13. *Al-Matari O. M. M., Helal I. M. A., Mazen Sh. A., Elhennawy Sh.* Adopting security maturity model to the organizations' capability model // Egyptian Informatics Journal. 2021. № 2 (22). P. 193–199.
14. *Muthukrishnan S. M., Palaniappan S.* Security metrics maturity model for operational security // Proc. IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, 2016. P. 101–106.
15. *Sulistyowati D., Handayani F., Suryanto Y.* Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS // International Journal on Informatics Visualization. 2020. № 4 (4). P. 225–230.
16. *Rabii A., Assoul S., Ouazzani Touhami K., Roudies O.* Information and cyber security maturity models: a systematic literature review // Information and Computer Security. 2020. № 4 (28). P. 627–644.
17. *Arenas E., Palomino J., Mansilla J.* Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications Based on ISO 27032 and NIST // Proc. IEEE XXX International Conference on Electronics, Electrical Engineering and Computing (INTERCON), Lima, 2023. P. 1–8.
18. ISO/IEC 27035-1:2023 Information technology. Information security incident management. Part 1: Principles and process.
19. ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. Методика оценки соответствия».
20. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

Иванов Андрей Валерьевич
к.т.н., доцент, заведующий кафедрой защиты информации, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. Карла Маркса 20), e-mail: andrej.ivanov@corp.nstu.ru, ORCID: 0000-0003-2002-8572.

Огнев Игорь Александрович
ассистент кафедры защиты информации, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. Карла Маркса 20), e-mail: i.ognev.2016@corp.nstu.ru, ORCID: 0000-0003-3884-7170.

Никрошкин Иван Владимирович
ассистент кафедры защиты информации, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. Карла Маркса 20), e-mail: i.nikroshkin@corp.nstu.ru, ORCID: 0000-0003-4824-7419.

Киселев Максим Алексеевич
лаборант кафедры защиты информации, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. Карла Маркса 20), e-mail: m.kiselev.2019@stud.nstu.ru, ORCID ID: 0009-0009-8248-2800.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Assessment of the Level of Trust in the Information Security Incident Management Process

Andrey V. Ivanov, Igor A. Ognev, Ivan V. Nikroshkin, Maxim A. Kiselev

Novosibirsk State Technical University (NSTU)

Abstract: The existing methods for assessing the level of trust in the information security incident management process and in the processes of information security event monitoring systems are extremely limited. These methods are based on an expert assessment and are periodic in nature with a long-time interval between assessments. The purpose of this study is to develop a methodology for assessing the level of trust in the information security incident management process, which is suitable for an automated assessment with minimal expert participation. As a result of the work, a methodology has been developed to assess the level of confidence in the information security incident management process, which includes a list of trust criteria and metrics for their assessment. The methodology is based on the SOMM methodology and GOST ISO/IEC 27035. The developed methodology is based on a three-stage assessment of trust indicators: assessment of trust metrics, assessment of trust criteria, assessment of the level of trust in the information incident management process.

Keywords: information security incidents, incident management, process assessment, level of trust, trust, information security, information security monitoring, cybersecurity.

For citation: Ivanov A. V., Ognev I. A., Nikroshkin I. V., Kiselev M. A. Assessment of the level of trust in the information security incident management process (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 88-102. https://doi.org/10.55648/1998-6920-2024-18-2-88-102.

The article was submitted: 09.02.2024; accepted for publication 29.02.2024.

References

1. Veligodskii S. S., Miloslavskaya N. G. Unifitsirovannaya model' zrelosti tsentrov upravleniya setevoi bezopasnost'yu informatsionno-telekommunikatsionnykh setei [Unified Maturity Model for Network Security Control Centers of Information and Telecommunication Networks]. *Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki*., 2023, no. 3 (233), pp. 157-172.
2. Seleznev V. M., Borovskaya O. E. Vstraivanie instrumentov SOAR-platform v ekosistemu SOC dlya avtomatizatsii protsessa reagirovaniya na intsidenty IB [Embedding SOAR platform tools into the SOC ecosystem to automate the process of responding to information security incidents]. *International Research Journa*l, 2022, no. 10 (124), pp. 1-9.
3. Verevkin S. A., Kravchuk A. V., Belyakov M. I. Metodika upravleniya intsidentami informatsionnoi bezopasnosti na ob"ektakh kriticheskoi informatsionnoi infrastruktury [Information Security Incident Management Methodology at Critical Information Infrastructure Facilities]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki*, 2022, no. 8, pp. 116-120.
4. Sukhov A. M. Otsenivanie effektivnosti protsessa funktsionirovaniya sistemy obespecheniya informatsionnoi bezopasnosti na osnove teorii stokhasticheskoi indikatsii [Evaluation of the Efficiency of the Information Security System Functioning Process Based on the Stochastic Indication Theory]. *Informatsionno-upravlyayushchie sistemy*, 2022, no. 3, pp. 31-44.
5. Ivanov A. V., Nikroshkin I. V., Ognev I. A., Kiselev M. A. Primenenie sredstv ekspertizy Blue Team v protsesse monitoringa informatsionnykh sistem na primere platformy TI (Threat Intelligence) [Application of the Blue Team expertise tools in the process of monitoring information systems on the example of the TI platform (Threat Intelligence)]. *Bezopasnost' tsifrovykh tekhnologii*, 2023, no. 2 (109), pp. 34-51. DOI: 10.17212/2782-2230-2023-2-34-51.
6. Reva I. L., Medvedev M. A., Vorontsova I. V. Issledovanie problematiki metodik opredeleniya tipa kontenta vo vkhodyashchem trafike [Study of the issues of methods for determining the type of content in incoming traffic]. *Sistemy analiza i obrabotki dannykh*, 2023, no. 4 (92), pp. 69-84. DOI: 10.17212/2782-2001-2023-4-69-84.
7. *Prikaz Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 11 fevralya 2013 g. N 17 "Ob utverzhdenii Trebovanii o zashchite informatsii, ne sostavlyayushchei gosudarstvennuyu tainu, soderzhashcheisya v gosudarstvennykh informatsionnykh sistemakh"* [Order of the Federal Service for Technical and Export Control No. 17 of February 11, 2013 "On Approval of the Requirements for the Protection of Information Not Constituting a State Secret Contained in State Information Systems"].
8. *Prikaz Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 18 fevralya 2013 g. N 21 "Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh* [Order of the Federal Service for Technical and Export Control No. 21 of February 18, 2013 "On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data During Their Processing in Personal Data Information Systems"].
9. *Prikaz Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 14 marta 2014 g. N 31 "Ob utverzhdenii Trebovanii k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"ektakh, potentsial'no opasnykh ob"ektakh, a takzhe ob"ektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudei i dlya okruzhayushchei prirodnoi sredy"* [Order of the Federal Service for Technical and Export Control No. 31 of March 14, 2014 "On Approval of the Requirements for Ensuring Information Security in Automated Control Systems for Production and Technological Processes at Critical Facilities, Potentially Hazardous Facilities, as well as Facilities Posing an Increased Danger to Human Life and Health and the Environment"].

10. *Prikaz Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 25 dekabrya 2017 g. N 239 "Ob utverzhdenii Trebovanii po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii"* [Order of the Federal Service for Technical and Export Control No. 239 of December 25, 2017 "On Approval of the Requirements for Ensuring the Security of Significant Facilities of the Critical Information Infrastructure of the Russian Federation"].
11. Selifanov V. V., Anikeeva V. V., Ognev I. A. Voprosy otsenki doveriya k sisteme upravleniya riskami [Issues of assessing the credibility of the risk management system]. Bezopasnost' tsifrovykh tekhnologii, 2023, no. 1 (108), pp. 69-82. DOI: 10.17212/2782-2230-2023-1-69-82.
12. Security Operations Maturity Model. *StarLink*, available at: `https://assets.starlinkme.net/gitex-vendor-assets/logrhythm/uk-security-operations-maturity-model-white-paper.pdf` (accessed: 30.01.2024).
13. Al-Matari O. M. M., Helal I. M. A., Mazen Sh. A., Elhennawy Sh. Adopting security maturity model to the organizations' capability model. *Egyptian Informatics Journal*., 2021, no. 2 (22), pp. 193-199.
14. Muthukrishnan S. M., Palaniappan S. Security metrics maturity model for operational security. *2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, IEEE Xplore, 2016, pp. 101-106.
15. Sulistyowati D., Handayani F., Suryanto Y. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *International Journal on Informatics Visualization*, 2020, vol 4, no. 4, pp. 225-230.
16. Rabii A., Assoul S., Ouazzani Touhami K., Roudies O. Information and cyber security maturity models: a systematic literature review. *Information and Computer Security*, 2020, vol.28, no. 4, pp. 627-644.
17. Arenas E., Palomino J., Mansilla J. Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications Based on ISO 27032 and NIST. *2023 IEEE XXX International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, Lima, IEEE Xplore, 2023, pp. 1-8.
18. *ISO/IEC 27035-1:2023 Information technology. Information security incident management. Part 1: Principles and process*.
19. *GOST R 57580.2-2018 «Bezopasnost' finansovykh (bankovskikh) operatsii. Zashchita informatsii finansovykh organizatsii. Bazovyi sostav organizatsionnykh i tekhnicheskikh mer. Metodika otsenki sootvetstviya»* [GOST R 57580.2-2018 "Security of Financial (Banking) Transactions. Protection of information of financial institutions. Basic composition of organizational and technical measures. Conformity Assessment Methodology"].
20. *GOST R 57580.1-2017 «Bezopasnost' finansovykh (bankovskikh) operatsii. Zashchita informatsii finansovykh organizatsii. Bazovyi sostav organizatsionnykh i tekhnicheskikh mer»* [GOST R 57580.1-2017 "Security of Financial (Banking) Transactions. Protection of information of financial institutions. Basic Composition of Organizational and Technical Measures"].

Andrey V. Ivanov

PhD in Technology, Head of the Department of Information Security, Associate Professor, Novosibirsk State Technical University, e-mail: `andrej.ivanov@corp.nstu.ru`, ORCID: 0000-0003-2002-8572.

Igor A. Ognev

Assistant of the Department of Information Security, Novosibirsk State Technical University (NSTU, 630073, Novosibirsk, Karl Marx Ave. 20), e-mail: `i.ognev.2016@corp.nstu.ru`, ORCID: 0000-0003-3884-7170.

Ivan V. Nikroshkin

Assistant of the Department of Information Security, Novosibirsk State Technical University (NSTU, 630073, Novosibirsk, Karl Marx Ave. 20), e-mail: `i.nikroshkin@corp.nstu.ru`, ORCID: 0000-0003-4824-7419.

Maksim A. Kiselev

Laboratory Assistant of the Department of Information Security, Novosibirsk State Technical University (NSTU, 630073, Novosibirsk, Karl Marx Ave. 20), e-mail: `m.kiselev.2019@stud.nstu.ru`, ORCID ID: 0009-0009-8248-2800.