

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
УЧРЕЖДЕНИЕ «ВСЕРОССИЙСКИЙ НАУЧНО-  
ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ  
МЕТРОЛОГИЧЕСКОЙ СЛУЖБЫ»  
(ФГБУ «ВНИИМС»)  
ФЕДЕРАЛЬНОГО АГЕНТСТВА ПО ТЕХНИЧЕСКОМУ  
РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ**

**УТВЕЖДАЮ**  
Директор ФГБУ «ВНИИМС»

Денисенко С.А.

«16» января 2024 г.

**РЕКОМЕНДАЦИЯ  
ГОСУДАРСТВЕННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ ЕДИНСТВА  
ИЗМЕРЕНИЙ**

**МЕТОДИКА ОЦЕНКИ УРОВНЯ РИСКА  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СРЕДСТВ ИЗМЕРЕНИЙ**

МИ 3681-2024

Начальник лаб. 009/1 ФГБУ «ВНИИМС»

  
личная подпись

А.Н. Паньков  
инициалы, фамилия

Москва,  
2024 г.

## **ПРЕДИСЛОВИЕ**

**РАЗРАБОТАНА** Федеральным государственным бюджетным учреждением «Всероссийский научно - исследовательский институт метрологической службы» (ФГБУ «ВНИИМС»)

**ИСПОЛНИТЕЛИ** Паньков А.Н., к.т.н., (руководитель темы); Лазарева И.В.

**УТВЕРЖДЕНА** ФГБУ «ВНИИМС» 16 января 2024 г.

**ЗАРЕГИСТРИРОВАНА** ФГБУ «ВНИИМС» 22 января 2024 г.

**ВВЕДЕНА ВПЕРВЫЕ**

## СОДЕРЖАНИЕ

|                                                                                |           |
|--------------------------------------------------------------------------------|-----------|
| <b>1 Область применения .....</b>                                              | <b>4</b>  |
| <b>2 Нормативные ссылки.....</b>                                               | <b>4</b>  |
| <b>3 Термины, определения и сокращения .....</b>                               | <b>5</b>  |
| <b>4 Общие положения .....</b>                                                 | <b>7</b>  |
| <b>5 Оценка уровня риска ИБ программного обеспечения .....</b>                 | <b>7</b>  |
| <b>5.1 Идентификация активов .....</b>                                         | <b>7</b>  |
| <b>5.2 Идентификация неблагоприятных воздействий .....</b>                     | <b>8</b>  |
| <b>5.3 Критерии оценки.....</b>                                                | <b>8</b>  |
| <b>5.4 Оценка неблагоприятных воздействий в соответствии с критериями.....</b> | <b>16</b> |
| <b>5.5 Оценка уровня риска ИБ ПО СИ.....</b>                                   | <b>17</b> |
| <b>6 Оформление результатов.....</b>                                           | <b>18</b> |
| <b>БИБЛИОГРАФИЯ .....</b>                                                      | <b>20</b> |

| Рекомендация                                                                                        | Группа Т 85  |
|-----------------------------------------------------------------------------------------------------|--------------|
| Государственная система обеспечения единства измерений                                              |              |
| Методика оценки уровня риска информационной безопасности программного обеспечения средств измерений | МИ 3681-2024 |

## 1 Область применения

1.1 Настоящая рекомендация распространяется на средства измерений с программным управлением и предназначена для оценки уровня риска информационной безопасности программного обеспечения средств измерений.

1.2 Рекомендация разработана с целью реализации положений Международного Документа МОЗМ D31 «Общие требования к средствам измерений с программным управлением» в части применения риск ориентированного подхода при испытаниях программного обеспечения средств измерений.

## 2 Нормативные ссылки

В рекомендации использованы ссылки на следующие нормативные документы:

ГОСТ Р 8.654-2015 Государственная система обеспечения единства измерений (ГСИ). Требования к программному обеспечению средств измерений. Основные положения;

ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности;

ГОСТ Р ИСО/МЭК 15408-2012 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий;

ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности.

OIML D 31 General requirements for software controlled measuring instruments. (Общие требования к средствам измерений с программным управлением).

### **3 Термины, определения и сокращения**

3.1 В настоящей рекомендации применены следующие термины с соответствующими определениями:

3.1.1 **данные:** Информация, представленная в виде, пригодном для передачи, интерпретации или обработки

[ГОСТ 8.654-2015. п.3.2]

3.1.2 **идентификационные данные (признаки) программного обеспечения:** Однозначно связанная с конкретным программным обеспечением последовательность символов (букв, цифр и т.п.), например, контрольная сумма.

[ГОСТ 8.654-2015. п.3.4]

3.1.3 **идентификация программного обеспечения:** Проверка и подтверждение подлинности и целостности программного обеспечения, выраженное в символах (буквах, цифрах), однозначно связанных с программным обеспечением (например, контрольная сумма).

[ГОСТ 8.654-2015. п.3.5]

3.1.4 **интерфейс:** Общая граница между двумя блоками (функциональными единицами), характеризующимися различными функциями, физическими соединениями и обменом сигналами.

[ГОСТ 8.654-2015. п.3.6]

3.1.5 **метрологически значимая часть ПО:** Программы и программные модули, выполняющие обработку измерительной информации и реализующие функции по идентификации и защите ПО СИ.

[ГОСТ 8.654-2015. п.3.11]

**3.1.6 ПО СИ:** Программы (совокупность программ), предназначенные для использования в СИ и реализующие в том числе сбор, передачу, обработку, хранение и представление измерительной информации, а также программные модули и компоненты, необходимые для функционирования этих программ.

[ГОСТ 8.654-2015. п.3.17]

**3.1.7 активы:** Объекты, подлинность, целостность или доступность данных, которые подлежат защите.

Примечание.

В случае ПО СИ к активам относятся метрологически значимая часть и данные измерений.

**3.1.8 злоумышленник:** Лицо или группа лиц, готовые манипулировать результатами измерений и измерительными инструментами.

**3.1.9 негативные действия:** Действия, выполняемые злоумышленником по отношению к активам.

**3.1.10 угроза:** Негативное действие, выполняемое источником угрозы (злоумышленником) по отношению к некоторому активу.

**3.1.11 уровня риска информационной безопасности программного обеспечения:** бальная экспертная оценка возможности возникновения угроз и потенциального воздействия на безопасность программного обеспечения средств измерений.

**3.1.12 уязвимости ПО:** Слабые места ПО, которые могут быть использованы для реализации определенных угроз.

**3.1.13 экспертная оценка:** Процедура получения оценки проблемы на основании мнения специалистов с целью дальнейшего принятия решения.

**3.2** В настоящей рекомендации применены следующие сокращения:

БД – база(ы) данных;

ИБ – информационная безопасность;

ИТ – информационные технологии;

МЗЧ – метрологически значимая часть;

НД – нормативный документ;

ОО – объект оценки;

ОС – операционная система;

ПО – программное обеспечение;

СИ – средства измерений.

## **4 Общие положения**

4.1 Под оценкой уровня риска ПО СИ понимается процесс, в рамках которого выявляются возможные риски информационной безопасности, проводится базовая экспертная оценка возможности возникновения угроз и потенциального воздействия на безопасность программного обеспечения средств измерений.

## **5 Оценка уровня риска ИБ программного обеспечения**

### **5.1 Идентификация активов**

5.1.1 На первом этапе оценки уровня риска ИБ ПО СИ необходимо идентифицировать активы – свойства ПО или объекты, нуждающихся в защите.

5.1.2 Нормативными документами, которые определяют такие свойства ПО, являются Федеральный закон № 102 «Об обеспечении единства измерений», Приказ Минпромторга России № 2905, Рекомендации по метрологии Р 50.2.077-2014.

5.1.3 Активами в случае программного обеспечения средств измерений могут являться данные измерений, метрологически значимая часть ПО, идентификатор ПО, метрологически значимые параметры, хранимые или передаваемые (их целостность и подлинность).

5.1.4 В процессе идентификации активов определяется перечень злоумышленников. Под злоумышленниками в общем случае понимаются все участники, которые так или иначе взаимодействуют с СИ и с одинаковой

мотивацией готовы манипулировать результатами измерений и ПО СИ. В эту категорию входят производители, продавцы средств измерений, а также пользователи или сторонние лица.

## **5.2 Идентификация неблагоприятных воздействий**

5.2.1 Для каждого актива, определенного согласно п.5.1.1, проводят анализ возможных неблагоприятных воздействий. Примерами таких воздействий могут быть:

- подбор пароля на СИ или его элемент (БД, ОС);
- аннулирование доступа к журналу событий;
- замена результатов измерений;
- замена МЗЧ ПО;
- внесение изменений в интерфейс связи и передачи информации;
  - нарушение связи;
  - внесение ложной информации;
  - перехват информационных сообщений;
- изменение параметров поверки, калибровки или настроек СИ и др.

5.2.2 Для каждого из неблагоприятных воздействий назначается индивидуальный балл воздействия от 1 до 5.

Поскольку предполагается, что все идентифицированные активы одинаково важны, назначается самый высокий балл (5). Меньшая оценка выбирается только в том случае, если воздействие применяется только к одному измерению или может быть легко обнаружено при наблюдении за СИ и взаимодействующими с ним людьми.

## **5.3 Критерии оценки**

5.3.1 Каждое выбранное в п. 5.2 неблагоприятное воздействие оценивают в соответствии с критериями:

- время, затрачиваемое на поиск уязвимости в ПО и её использование (общее затрачиваемое время);
- требующаяся техническая компетентность специалиста (компетентность специалиста);
- знание объекта и его функционирования (знание объекта);
- возможность доступа к объекту;
- аппаратные средства/программное обеспечение ИТ или другое оборудование, требуемое для использования уязвимости;
- время, требуемое на восстановления работоспособности ПО СИ после сбоев и время, затрачиваемое на восстановление утраченных (изменённых, дискредитируемых) данных.

5.3.2 Во многих случаях эти факторы не являются независимыми и могут в различной степени заменять друг друга. Например, компетентность или аппаратные средства/программное обеспечение могут быть заменой времени. Эти факторы обсуждаются далее (уровни каждого фактора рассматриваются в порядке увеличения). В таком случае в фазе использования уязвимости рассматривается наименее «затратная» комбинация факторов.

5.3.3 Общее затрачиваемое время – это время, которое необходимо нарушителю для поиска потенциальной уязвимости, которая может существовать в ОО, разработки метода взлома нападения и поддержания усилий по осуществлению нападения на объект оценки. При рассмотрении данного фактора для определения, требуемого нарушителю количества времени, используется пессимистичный, наиболее неблагоприятный сценарий.

Принято выделять следующие уровни отрезков времени:

- a) менее одного дня;
- b) от одного дня до недели;
- c) от одной до двух недель;
- d) от двух недель до месяца;

е) месяц, два месяца, три - каждый дополнительный месяц до шести означает увеличение значения;

ф) более шести месяцев.

#### 5.3.4 Компетентность специалиста

Компетентность специалиста включает в себя уровень общих знаний основополагающих принципов или методов осуществления взлома ПО СИ. Здесь выделяют следующие типы специалистов:

- а) непрофессионалы слабо осведомлены по сравнению с экспертами или профессионалами, и не обладают специфической компетентностью
- б) профессионалы хорошо осведомлены в том, что касается режима безопасности продукта или системы данного типа;
- в) эксперты хорошо знакомы с основными алгоритмами, протоколами, аппаратными средствами, структурами, режимом безопасности, с применяемыми принципами и концепциями безопасности, а также с методами и средствами определения новых атак, криптографическими средствами и методами, классическими атаками на данный тип продукта ИТ, методами нападения и т. п., реализуемыми для данного типа продукта или системы;
- г) уровень «Эксперт в нескольких областях знаний или группа экспертов» применяется в случае, когда для осуществления отдельных этапов нападения необходимы знания на уровне Эксперт в различных областях.

В случае, когда требуется применить в описании несколько различных типов компетентности, то по умолчанию выбирается самый высокий уровень компетентности.

В некоторых особых случаях применимо значение уровня «Эксперт в нескольких областях знаний или группа экспертов», но в этом случае необходимо отметить, что области знаний, в которых предполагаемые нарушители являются экспертами, должны быть принципиально разными,

например, управление аппаратными средствами и криптография.

### 5.3.5 Знание объекта оценки

Знание объекта оценки указывает на определенный уровень знаний об объекте оценки. Оно отличается от общей компетентности, хотя и связано с ней. Выделяют следующие уровни знаний об объекте оценки:

а) общедоступная информация об ОО (например, полученная из сети Интернет);

б) информация ограниченного доступа об ОО (например, сведения, которыми управляет организация-разработчик и предоставляет их другим организациям на условиях соглашения о неразглашении информации);

с) чувствительная информация об ОО (например, сведения, которыми обладают закрытые рабочие группы организации-разработчика, и доступ, к которым имеют только члены данных групп);

д) критически важная информация об ОО (например, сведения, которые известны только нескольким лицам, и доступ к которым строго контролируется на основе личной ответственности и необходимости доступа для выполнения рабочих обязанностей).

Уровень знания об объекте оценки может различаться еще и в зависимости от детализации проекта ОО, хотя это осуществимо только на уровне описания основ ОО. Некоторые проекты объектов оценки могут представлять собой общедоступную информацию (или сильно зависящую от общедоступной) и поэтому даже представление проекта будет классифицироваться как общедоступная информация или, в крайнем случае, как информация ограниченного доступа, тогда как доступ к представлению реализации других ОО будет строго контролироваться, т.к. злоумышленник может получить из него сведения, которые могут помочь ему в осуществлении атаки, и поэтому такие представления реализации будут считаться чувствительной или даже критически важной информацией.

Бывают ситуации, когда требуется применить в описании несколько различных типов знания. По умолчанию выбирается самый высокий уровень факторов знания об ОО.

### 5.3.6 Возможность доступа к объекту оценки

Возможность доступа к объекту оценки имеет отношение к п. 5.3.3 «Общее затрачиваемое время». Идентификация или использование уязвимости могут требовать продолжительного доступа к объекту оценки, что может увеличить вероятность обнаружения. Некоторые методы совершения неблагоприятного воздействия могут требовать значительных автономных усилий без подключения к объекту оценки и лишь краткого времени доступа к ОО для использования уязвимости. Может также потребоваться непрерывный доступ или доступ в виде нескольких сеансов.

Для некоторых объектов оценки возможность доступа к ним может равняться числу образцов этих объектов, которые может получить злоумышленник.

Оценка возможности доступа к объекту оценки производится в соответствии с следующими категориями:

а) «отсутствие необходимости в доступе/неограниченный доступ» означает, что для нападения не важна возможность доступа к ОО, т. к. нет опасности обнаружения при осуществлении доступа к ОО и нет препятствий для доступа к образцам ОО для нападения;

б) «простой доступ» означает, что доступ требуется менее чем на день, а количество образцов ОО, к которым требуется доступ для осуществления нападения, меньше десяти;

с) «умеренная возможность доступа» означает, что доступ требуется менее чем на месяц, а количество образцов ОО, к которым требуется доступ для осуществления нападения, меньше сотни;

д) «затруднительный доступ» означает, что доступ требуется хотя бы на

месяц, а количество образцов ОО, к которым требуется доступ для осуществления нападения, больше или равно ста;

е) «невозможность доступа» означает, что времени возможности доступа недостаточно для осуществления нападения (промежуток времени, во время которого актив, на который направлено нападение, доступен или уязвим, меньше, чем промежуток времени, требуемый для осуществления нападения). Например, криптографический ключ некоторого актива меняется раз в неделю, а для его успешного подбора требуются две недели. Другой подобный случай — когда достаточное для осуществления нападения количество образцов ОО недоступно нарушителю — например если ОО является аппаратным средством, и вероятность его разрушения в процессе нападения больше, чем вероятность успешного завершения нападения, а у нарушителя есть всего один образец ОО.

#### 5.3.7. Аппаратные средства/программное обеспечение ИТ

Аппаратные средства/ПО ИТ или другое оборудование представляют собой оборудование, которое требуется для идентификации или использования уязвимости. Здесь выделяются следующие категории:

- Стандартное оборудование – это оборудование либо для идентификации уязвимости, либо для неблагоприятного воздействия, которое легко доступно нарушителю. Это оборудование может быть частью самого объекта оценки (например, отладчик в операционной системе) или может быть легко получено (например, программное обеспечение, загружаемое из Интернета, анализаторы протоколов или простые сценарии нападения).

- Специализированное оборудование, которое не слишком легко получить нарушителю, но может быть приобретено без значительных усилий. Это может быть покупка небольшого количества оборудования (например, средств атаки по энергопотреблению, использование сотни ПК, объединенных через сеть Интернет) или разработка более сложных сценариев и программ нападения. Если для проведения различных этапов нападения требуются

различные испытательные стенды со специальным оборудованием, это расценивается как заказное оборудование.

- Заказное оборудование, недоступное широкому кругу пользователей, поскольку для него либо может потребоваться специальная разработка (например, очень сложного программного обеспечения), либо оборудование настолько специализировано, что его распространение контролируется и, возможно, это оборудование является оборудованием ограниченного распространения. Или же данное оборудование очень дорогостоящее.

- Несколько видов заказного оборудования применяется в том случае, когда для осуществления отдельных этапов нападения необходимо различное, сделанное на заказ оборудование.

5.3.8 Время восстановления работоспособности ПО и время восстановления утраченных (изменённых, дискредитируемых) данных.

Время восстановления работоспособности ПО СИ и время восстановления утраченных или измененных данных являются критическими параметрами в обеспечении безопасности СИ с программным управлением. Чем меньше это время, тем менее вероятно возникновение серьезных последствий в случае уязвимости или инцидента.

Время восстановления работоспособности программного обеспечения – время, необходимое для восстановления нормальной работы ПО СИ после сбоя или атаки. Если восстановление происходит быстро, это помогает сократить потери в производительности и уменьшить воздействие на измерительные процессы.

Время восстановления утраченных данных – время, необходимое для восстановления данных после их потери, изменения или уничтожения. Эффективное восстановление данных позволяет минимизировать потери информации и предотвращает серьезные последствия для экономики.

Обеспечение минимального времени восстановления является ключевым элементом стратегии информационной безопасности программного обеспечения. Организации стремятся разрабатывать и поддерживать меры для быстрого восстановления после инцидентов. В этом контексте выделяются следующие категории:

- а) «Восстановление работоспособности или утраченных данных невозможно». В случае серьезной угрозы безопасности или критического повреждения данных процесс восстановления становится невозможным. Например, при разрушении данных без возможности их восстановления.
- б) «Очень длительное время восстановления» Требуется несколько недель или более. Это включает сложную диагностику, возможно, восстановление данных с участием специализированных команд и оборудования.
- в) «Длительное время восстановления» От нескольких дней до недели. Требуется более глубокая диагностика, возможно, восстановление данных с использованием специализированных инструментов.
- г) «Среднее время восстановления» От нескольких часов до дня. Восстановление может потребовать более тщательной диагностики, возможно, восстановление данных из резервных копий.
- е) «Минимальное время восстановления» Несколько часов или менее. Восстановление осуществляется либо из резервных копий, либо путем быстрой диагностики и устранения проблемы. Оперативное восстановление минимизирует временные потери и обеспечивает быстрое восстановление работоспособности системы.

## 5.4 Оценка неблагоприятных воздействий в соответствии с критериями

5.4.1 В зависимости от сложности реализации неблагоприятного воздействия по каждому из идентифицированных ранее критериев методом экспертных оценок вычисляется средний балл, причем, количество привлекаемых экспертов обычно составляет 5-12 человек, а средний балл вычисляется с учетом уровня компетенции каждого из экспертов.

Чем больше средний балл, тем сложнее совершить воздействие, соответственно, тем выше сопротивляемость ПО к воздействию. Численные значения выбирать из предложенных в таблице 1.

Таблица 1

| Критерий                  |                                                          | Значение |
|---------------------------|----------------------------------------------------------|----------|
| Общее затрачиваемое время | $\leq 1$ день                                            | 0        |
|                           | $\leq 1$ неделя                                          | 1        |
|                           | $\leq 2$ недели                                          | 2        |
|                           | $\leq 1$ месяц                                           | 4        |
|                           | $\leq 2$ месяца                                          | 7        |
|                           | $\leq 3$ месяца                                          | 10       |
|                           | $\leq 4$ месяца                                          | 13       |
|                           | $\leq 5$ месяцев                                         | 15       |
|                           | $\leq 6$ месяцев                                         | 17       |
|                           | $> 6$ месяцев                                            | 19       |
| Компетентность            | Непрофессионал                                           | 0        |
|                           | Профессионал                                             | 3        |
|                           | Эксперт                                                  | 6        |
|                           | Группа экспертов                                         | 8        |
| Знание ОО                 | Общедоступная информация                                 | 0        |
|                           | Информация ограниченного доступа                         | 3        |
|                           | Чувствительная информация                                | 7        |
|                           | Критически важная информация                             | 11       |
| Возможность доступа к ОО  | Отсутствие необходимости в доступе/неограниченный доступ | 0        |
|                           | Простой доступ                                           | 1        |
|                           | Умеренная возможность доступа                            | 4        |
|                           | Затруднительный доступ                                   | 10       |
|                           | Невозможность доступа                                    | $\infty$ |
| Оборудование              | Стандартное                                              | 0        |
|                           | Специализированное                                       | 4        |
|                           | Сделанное на заказ                                       | 7        |
|                           | Несколько видов сделанного на заказ оборудования         | 9        |
| Время восстановления      | Восстановление невозможно                                | 0        |

| Критерий                                                                                                                |                                       | Значение |
|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------|----------|
| работоспособности ПО и время восстановления утраченных (изменённых, дискредитируемых) данных                            | Очень длительное время восстановления | 4        |
|                                                                                                                         | Длительное время восстановления       | 9        |
|                                                                                                                         | Среднее время восстановления          | 15       |
|                                                                                                                         | Минимальное время восстановления      | 19       |
| ∞ указывает, что атаку невозможно осуществить из-за предпринятых других мер в предполагаемой среде функционирования ОО. |                                       |          |

## 5.5 Оценка уровня риска ИБ ПО СИ

5.5.1 Вычислить общую сумму баллов, полученных в п.5.4 настоящей методики.

5.5.2 Соотнести полученное значение со значениями, приведенными в таблице 1. Таким образом получаем значение уровня стойкости ОО к потенциально возможному несанкционированному влиянию на МЗЧ ПО СИ и данные измерений.

Таблица 2

| Диапазон значений | Уровень стойкости ОО |
|-------------------|----------------------|
| 0-9               | Не противостоит      |
| 10-13             | Базовый              |
| 14-19             | Усиленный базовый    |
| 20-24             | Умеренный            |
| $\geq 25$         | Высокий              |

5.5.3 Полученное значение рейтинга воздействия сопоставляют с оценкой между 1 и 5, где 5 представляет высокую вероятность возникновения для неблагоприятного воздействия, а 1 указывает, что оно очень маловероятно. Эти значения приведены в таблице 3.

Таблица 3

| Сумма баллов | Оценка сопротивления | Уровень риска |
|--------------|----------------------|---------------|
| 0-9          | Не противостоит      | 5             |
| 10-13        | Базовый              | 4             |
| 14-19        | Усиленный базовый    | 3             |
| 20-24        | Умеренный            | 2             |
| $\geq 25$    | Высокий              | 1             |

5.5.4 Значение оценки риска ИБ, связанного с реализацией **неблагоприятного воздействия**, вычислить путем умножения значения оценки воздействия (от 1 до 5) для данного воздействия на уровень риска наиболее вероятного неблагоприятного воздействия. Это выражение представлено формулой 1:

$$\text{Оценка риска} = \frac{\text{Оценка воздействия} * \text{Уровень риска}}{5} \quad (1)$$

## **6 Оформление результатов**

6.1 Результаты оценки уровня риска ИБ ПО СИ оформляют отдельным протоколом. Пример оформления результатов приведен в Приложении 1 настоящей рекомендации.

## Оценка уровня риска информационной безопасности программного обеспечения средства измерений

| Критерий                   | Неблагоприятное воздействие                                                              |                                                                                                     |                                                                                |
|----------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
|                            | Удаленный доступ злоумышленника к личному кабинету с помощью подбора пароля и замена МЗЧ | Доступ злоумышленника к промышленному компьютеру и изменение измерительной информации в базе данных | Удаленный доступ злоумышленника к веб-серверу и изменение параметров измерений |
| Затраченное время          | 10                                                                                       | 2                                                                                                   | 7                                                                              |
| Компетентность специалиста | 3                                                                                        | 3                                                                                                   | 6                                                                              |
| Знание ОО                  | 3                                                                                        | 0                                                                                                   | 3                                                                              |
| Возможность доступа к ОО   | 4                                                                                        | 10                                                                                                  | 4                                                                              |
| Оборудование               | 0                                                                                        | 0                                                                                                   | 0                                                                              |
| <b>Сумма баллов</b>        | <b>20</b>                                                                                | <b>15</b>                                                                                           | <b>20</b>                                                                      |
| <b>Уровень риска</b>       | <b>2</b>                                                                                 | <b>3</b>                                                                                            | <b>2</b>                                                                       |
| <b>Оценка риска</b>        | <b>2</b>                                                                                 | <b>3</b>                                                                                            | <b>2</b>                                                                       |

Оценка уровня риска ИБ ПО СИ будет равна 3 (максимальная оценка по всем критериям), а наиболее вероятным неблагоприятным воздействием будет доступ злоумышленника к промышленному компьютеру и изменение измерительной информации в базе данных.

## **БИБЛИОГРАФИЯ**

1. OIML D 31 Edition 2023 (E) General requirements for software controlled measuring instruments. (Общие требования к программно-контролируемым средствам измерений).
2. ГОСТ Р 8.839-2013 ГСИ. Общие требования к измерительным приборам с программным управлением. М., 2014
3. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011
4. ГОСТ Р ИСО/МЭК 15408-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. М., 2014
5. Р 50.2.077-2014 ГСИ. Испытания средств измерений в целях утверждения типа. Проверка защиты программного обеспечения. М., 2014