МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**



**МОСКОВСКИЙ**

**ПОЛИТЕХ**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Информационная безопасность»

Проектная деятельность

Тема: “**Оценка зрелости процессов ИБ в соответствии с фреймворком NIST Cybersecurity Framework**”

Выполнил: Студент 2 курса гр. 191-352

Валявский Алексей Александрович

Научный руководитель:

Агеева Елена Александровна

2021 г. Москва

**Фреймворк NIST Cybersecurity Framework**

В целом весь Фреймворк состоит из 3 основных элементов:

1. Ядро (the Framework Core)
2. Профили (the Framework Profile)
3. Уровни реализации (the Framework Implementation Tiers)

**1 Ядро** представляет собой набор активностей и информативных ссылок по ИБ, общий для некоторого набора критических ресурсов.

**Элементы ядра Фреймворка взаимодействуют следующим образом:  
Функции** систематизируют базовые активности ИБ на самом высоком уровне абстракции. Например, как указано на рисунке: идентификация, защита, обнаружение, реагирование и восстановление. На данный момент определены только эти базовые Функции. Включение других важных Функций включено в план развития Фреймворка.  
**Категории**являются подразделами Функций тесно связанными с практическими нуждами и реальными мероприятиями. Например: управление активами, контроль доступа, обнаружение вторжений.  
**Подкатегории** представляют собой дальнейшее деление Категорий, но не являются исчерпывающим набором активностей данной Категории. Например: «физические активы организации подвергаются инвентаризации», «сбор оповещений со всех систем производится централизованно в единой системе».  
**Информативные ссылки** указывают на конкретные разделы руководств, практик и стандартов, иллюстрирующие методы выполнения конкретных активностей.

**2** Профили являются инструментом, позволяющим организации определить последовательность устранения рисков ИБ в соответствии с задачами всей организации и отдельных её структурных подразделений, учитывающим требования законодательства, регуляторов и лучших практик, а также отражающим приоритеты процесса управления рисками. Профили могут быть использованы для описания как текущего, так и целевого статуса ИБ, что позволяет обнаружить недостатки для дальнейшего устранения рисков ИБ. Целевой профиль создаётся для отражения требований ИБ, предъявляемых к бизнесу, и может использоваться при взаимодействии между организациями по вопросам ИБ.

#### Уровни реализации (the Framework Implementation Tiers)

Уровни реализации Фреймворка показывают, как в организации осуществляется управление рисками ИБ. Уровни начинаются с Частичного (1 уровень) и заканчиваются Адаптивным (4 уровень) и описывают строгость и сложность применяемых практик управления рисками ИБ и в какой степени управление рисками ИБ интегрировано в общий процесс управления рисками.

Уровень 1: **Частичный**

Процесс управления рисками не формализован и осуществляется по обстановке, в том числе в манере реагирования на инциденты ИБ. Отсутствует подход в масштабах всей организации к управлению рисками ИБ. Организация может не принимать участия в координации или взаимодействии с другими субъектами по вопросам ИБ.

Уровень 2: **Информированный о рисках**

Управление рисками утверждено, но может не осуществляться в масштабах всей организации. Уделяется внимание управлению рисками ИБ, но отсутствует единый подход в масштабах всей организации. Организация осознаёт свою роль в общей экосистеме, но не формализует процессы взаимодействия с другими субъектами по вопросам ИБ.

Уровень 3: **Информированный о рисках и повторяемый**

Управление рисками утверждено и оформлено в виде политик, осуществляется регулярный анализ и пересмотр применяемых практик. Применяется единый подход к управлению рисками ИБ в масштабах всей организации. Организация осуществляет обмен информацией с другими субъектами.

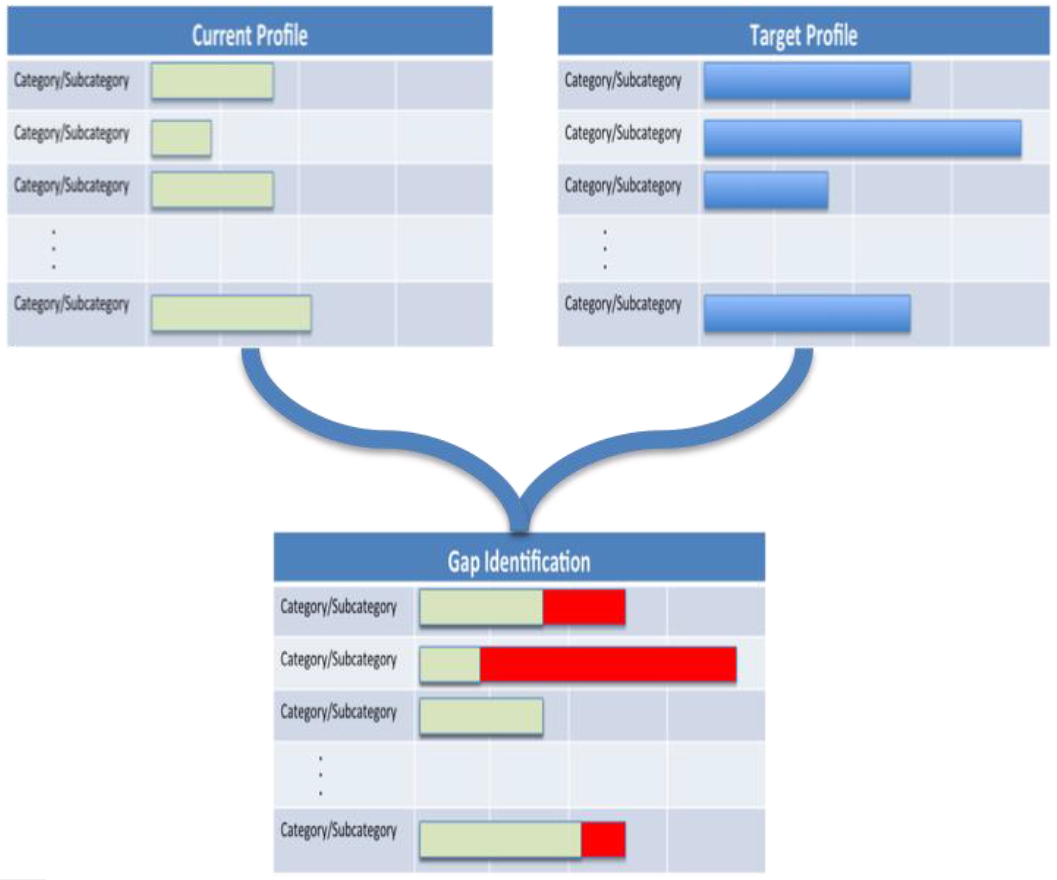
Уровень 4:**Адаптивный**

Организация актуализирует практики ИБ, основываясь на опыте предыдущих активностей по ИБ, и, непрерывно улучшая процесс управления рисками ИБ, адаптируется к изменениям обстановки в сфере ИБ. Применяется единый подход к управлению рисками ИБ в масштабах всей организации, превращающий этот процесс в часть корпоративной культуры. Организация активно осуществляет обмен информацией с другими субъектами для улучшения ИБ до наступления инцидентов.

**Подходы к оценке зрелости процессов ИБ.**

Для анализа зрелости ИБ в фреймворке существуют **профили**.

Профили - это уникальное согласование организацией своих организационных требований и целей, склонности к риску и ресурсов с желаемыми результатами ядра структуры. Профили могут использоваться для определения возможностей улучшения положения в области кибербезопасности путем сравнения “текущего” профиля с “целевым” профилем.

1 Действующий профиль ИБ

2 Целевой профиль ИБ

3 Разница в профилях, которую в дальнейшем необходимо свести к минимуму.

**Организации, которые могут пользоваться данным фреймворком.**

На сайте, на котором представлен данный фреймворк написано, что данный фреймворк универсален для компаний всех размеров и направлений.

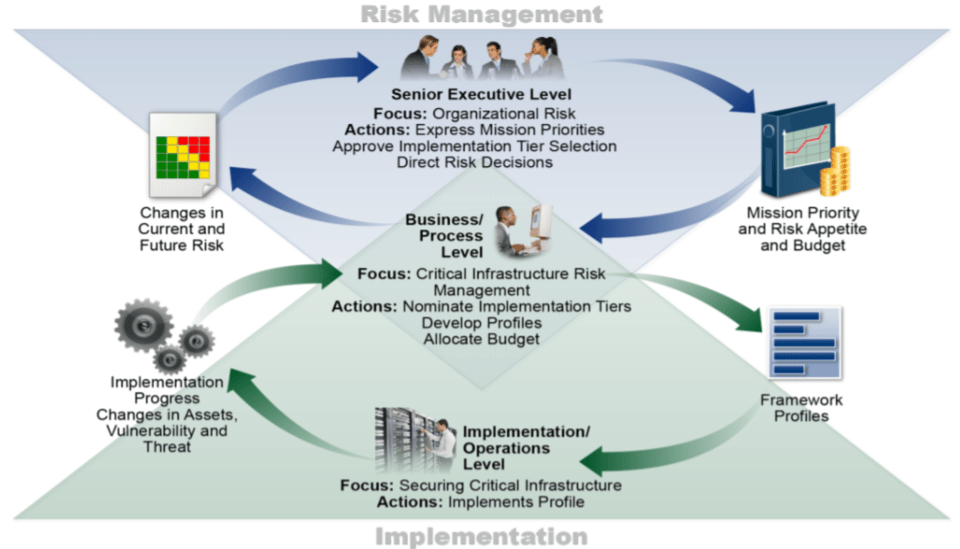
«***Система кибербезопасности предназначена для организаций всех размеров, секторов и сроков погашения.***

***Хотя фреймворк был разработан с учетом критической инфраструктуры (ки), он чрезвычайно универсален.***

***С помощью встроенных механизмов настройки (*например*, уровни, профили и ядро могут быть изменены) фреймворк может быть настроен для использования любым типом организации.****»*

#### ****Поддержка управления рисками с помощью фреймворка****

Эта структура помогает направлять ключевые моменты принятия решений о деятельности по управлению рисками на различных уровнях организации - от высшего руководства до уровня бизнеса и процессов, а также внедрения и операций.



Исполнительный уровень передает приоритеты миссии, имеющиеся ресурсы и общую толерантность к риску на уровень бизнес-процессов. Уровень бизнес-процесса использует информацию в качестве входных данных в процесс управления рисками, а затем формирует профиль для координации деятельности по внедрению/эксплуатации. Уровень внедрения / операций связывает прогресс внедрения профиля с уровнем бизнес-процессов. Уровень бизнес-процессов использует эту информацию для проведения оценки воздействия. Руководство на уровне бизнеса / процессов сообщает результаты этой оценки воздействия исполнительному уровню для информирования общего процесса управления рисками организации и уровню внедрения / операций для повышения осведомленности о влиянии бизнеса.

**Основные функции.**

NIST Cybersecurity Framework включает в себя набор функций, посредством которых осуществляется:

1. **Идентификация объектов системы.**
2. **Защита объектов системы.**
3. **Обнаружение угроз.**
4. **Реагирование на инциденты.**
5. **Процесс восстановления системы.**

Каждая из функций в свою очередь подразделяется на категории и подкатегории.

1. **Идентификация объектов системы.** Identification(ID)**.**

Идентификация объектов проводится с целью составления перечня объектов , которые необходимо защищать.

* 1. **Asset Management (ID.AM):** Данные, персонал, устройства, системы и средства, которые позволяют организации достичь бизнес-целей, идентифицируются и управляются в соответствии с их относительной важностью для целей организации и стратегии управления рисками организации.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты.** |
| **ID.AM-1:** Инвентаризация физических устройств и систем в организации | **CIS CSC** 1 |
| **COBIT 5** BAI09.01, BAI09.02 |
| **ISA 62443-2-1:2009** 4.2.3.4 |
| **ISA 62443-3-3:2013** SR 7.8 |
| **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 |
| **NIST SP 800-53** **Rev. 4** CM-8, PM-5 |
| **ID.AM-2:** Инвентаризация программных платформ и приложений в организации | **CIS CSC** 2 |
| **COBIT 5** BAI09.01, BAI09.02, BAI09.05 |
| **ISA 62443-2-1:2009** 4.2.3.4 |
| **ISA 62443-3-3:2013** SR 7.8 |
| **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 |
| **NIST SP 800-53** **Rev. 4** CM-8, PM-5 |
| **ID.AM-3:** Отображаются организационные коммуникации и потоки данных | **CIS CSC** 12 |
| **COBIT 5** DSS05.02 |
| **ISA 62443-2-1:2009** 4.2.3.4 |
| **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 |
| **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 |
| **ID.AM-4:** Каталогизированы внешние информационные системы. | **CIS CSC** 12 |
| **COBIT 5** APO02.02, APO10.04, DSS01.02 |
| **ISO/IEC 27001:2013** A.11.2.6 |
| **NIST SP 800-53** **Rev. 4** AC-20, SA-9 |
| **ID.AM-5:** Ресурсы (например, оборудование, устройства, данные, время, персонал и программное обеспечение) распределяются по приоритетам на основе их классификации, важности и ценности для бизнеса. | **CIS CSC** 13, 14 |
| **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 |
| **ISA 62443-2-1:2009** 4.2.3.6 |
| **ISO/IEC 27001:2013** A.8.2.1 |
| **NIST SP 800-53** **Rev. 4** CP-2, RA-2, SA-14, SC-6 |
| **ID.AM-6:** Установлены роли и обязанности в области кибербезопасности для всего персонала и сторонних заинтересованных сторон (например, поставщиков, клиентов, партнеров). | **CIS CSC** 17, 19 |
| **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 |
| **ISA 62443-2-1:2009** 4.3.2.3.3 |
| **ISO/IEC 27001:2013** A.6.1.1 |
| **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11 |

* 1. **Business Environment (ID.BE):** Миссии, цели, заинтересованные стороны и деятельность организации понятны и расставлены по приоритетам; эта информация используется для информирования о ролях, обязанностях и решениях по управлению рисками в области кибербезопасности.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **ID.BE-1:** Роль организации в цепочке поставок определяется и доводится до сведения | **COBIT 5** APO08.01,APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 |
| **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 |
| **NIST SP 800-53** **Rev. 4** CP-2, SA-12 |
| **ID.BE-2:** Место организации в критической инфраструктуре и ее отраслевом секторе определяется и сообщается | **COBIT 5** APO02.06, APO03.01 |
| **ISO/IEC 27001:2013** Clause 4.1 |
| **NIST SP 800-53** **Rev. 4** PM-8 |
| **ID.BE-3:** Приоритеты для миссии, целей и деятельности организации устанавливаются и сообщаются | **COBIT 5** APO02.01, APO02.06, APO03.01 |
| **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 |
| **NIST SP 800-53** **Rev. 4** PM-11, SA-14 |
| **ID.BE-4:** Установлены зависимости и критические функции для предоставления критически важных услуг. | **COBIT 5** APO10.01, BAI04.02, BAI09.02 |
| **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 |
| **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14 |
| **ID.BE-5:** Требования к устойчивости для поддержки предоставления критически важных услуг установлены для всех рабочих состояний (например, под давлением / атакой, во время восстановления, нормальной эксплуатации) | **COBIT 5** BAI03.02,DSS04.02 |
| **ISO/IEC 27001:2013** A.11.1.4,A.17.1.1,A.17.1.2, A.17.2.1 |
| **NIST SP 800-53** **Rev. 4** CP-2, CP-11, SA-13, SA-14 |

* 1. **Governance (ID.GV):** Политики, процедуры и процессы для управления и мониторинга нормативных, юридических, рисковых, экологических и операционных требований организации понятны и информируют руководство по рискам кибербезопасности.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **ID.GV-1:** Установлена ​​и доведена до сведения организационная политика кибербезопасности | **CIS CSC** 19 |
| **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 |
| **ISA 62443-2-1:2009** 4.3.2.6 |
| **ISO/IEC 27001:2013** A.5.1.1 |
| **NIST SP 800-53** **Rev. 4** -1 controls from all security control families |
| **ID.GV-2:** Роли и обязанности в области кибербезопасности координируются и согласовываются с внутренними ролями и внешними партнерами | **CIS CSC** 19 |
| **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 |
| **ISA 62443-2-1:2009** 4.3.2.3.3 |
| **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 |
| **NIST SP 800-53** **Rev. 4** PS-7,PM-1, PM-2 |
| **ID.GV-3:** Правовые и нормативные требования в отношении кибербезопасности, включая обязательства по соблюдению конфиденциальности и гражданских свобод, понятны и управляются | **CIS CSC** 19 |
| **COBIT 5** BAI02.01,MEA03.01, MEA03.04 |
| **ISA 62443-2-1:2009** 4.4.3.7 |
| **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 |
| **NIST SP 800-53** **Rev. 4** -1 controls from all security control families |
| **ID.GV-4:** Процессы корпоративного управления и управления рисками направлены на устранение рисков кибербезопасности | **COBIT 5** EDM03.02, APO12.02, APO12.05,DSS04.02 |
| **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 |
| **ISO/IEC 27001:2013** Clause 6 |
| **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 |

* 1. **Risk Assessment (ID.RA):** Организация осознает риск кибербезопасности для операций организации (включая миссию, функции, имидж или репутацию), активов организации и отдельных лиц.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **ID.RA-1:** Уязвимости активов выявляются и документируются | **CIS CSC** 4 |
| **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 |
| **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 |
| **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 |
| **NIST SP 800-53** **Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 |
| **ID.RA-2:** Информация о киберугрозах получена с форумов и источников по обмену информацией | **CIS CSC** 4 |
| **COBIT 5** BAI08.01 |
| **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 |
| **ISO/IEC 27001:2013** A.6.1.4 |
| **NIST SP 800-53** **Rev. 4** SI-5, PM-15, PM-16 |
| **ID.RA-3:** Выявление и документирование угроз, как внутренних, так и внешних. | **CIS CSC** 4 |
| **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 |
| **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 |
| **ISO/IEC 27001:2013** Clause 6.1.2 |
| **NIST SP 800-53** **Rev. 4** RA-3, SI-5, PM-12, PM-16 |
| **ID.RA-4:** Выявлены потенциальные последствия для бизнеса и вероятность | **CIS CSC** 4 |
| **COBIT 5** DSS04.02 |
| **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 |
| **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 |
| **NIST SP 800-53** **Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11 |
| **ID.RA-5:** Угрозы, уязвимости, вероятности и воздействия используются для определения риска. | **CIS CSC** 4 |
| **COBIT 5** APO12.02 |
| **ISO/IEC 27001:2013** A.12.6.1 |
| **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16 |
| **ID.RA-6:** Ответы на риски определены и приоритизированы | **CIS CSC** 4 |
| **COBIT 5** APO12.05, APO13.02 |
| **ISO/IEC 27001:2013** Clause 6.1.3 |
| **NIST SP 800-53 Rev. 4** PM-4, PM-9 |

* 1. **Risk Management Strategy (ID.RM):** Приоритеты, ограничения, допустимые пределы риска и допущения организации устанавливаются и используются для поддержки решений по операционным рискам.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **ID.RM-1:** Процессы управления рисками устанавливаются, управляются и согласовываются заинтересованными сторонами организации. | **CIS CSC** 4 |
| **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 |
| **ISA 62443-2-1:2009** 4.3.4.2 |
| **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 |
| **NIST SP 800-53** **Rev. 4** PM-9 |
| **ID.RM-2:** Толерантность к организационному риску определена и четко выражена | **COBIT 5** APO12.06 |
| **ISA 62443-2-1:2009** 4.3.2.6.5 |
| **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 |
| **NIST SP 800-53** **Rev. 4** PM-9 |
| **ID.RM-3:** Определение терпимости к риску определяется ее ролью в критической инфраструктуре и анализе рисков в конкретном секторе. | **COBIT 5** APO12.02 |
| **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 |
| **NIST SP 800-53 Rev. 4** SA-14,PM-8, PM-9, PM-11 |

* 1. **Supply Chain Risk Management (ID.SC):** Приоритеты, ограничения, допустимые пределы риска и допущения организации устанавливаются и используются для поддержки решений о рисках, связанных с управлением рисками в цепочке поставок. Организация установила и внедрила процессы для выявления, оценки и управления рисками цепочки поставок.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **ID.SC-1:** Процессы управления рисками цепочки киберпоставок выявляются, устанавливаются, оцениваются, управляются и согласовываются с заинтересованными сторонами организации. | **CIS CSC** 4 |
| **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 |
| **ISA 62443-2-1:2009** 4.3.4.2 |
| **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 |
| **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9 |
| **ID.SC-2:** Поставщики и сторонние партнеры информационных систем, компонентов и услуг выявляются, устанавливаются приоритеты и оцениваются с использованием процесса оценки рисков цепочки поставок в киберпространстве. | **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 |
| **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 |
| **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 |
| **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9 |
| **ID.SC-3:** Контракты с поставщиками и сторонними партнерами используются для реализации соответствующих мер, направленных на достижение целей программы кибербезопасности организации и Плана управления рисками цепочки поставок в киберпространстве. | **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 |
| **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 |
| **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 |
| **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9 |
| **ID.SC-4:** Поставщики и сторонние партнеры обычно оцениваются с использованием аудитов, результатов испытаний или других форм оценки для подтверждения того, что они выполняют свои договорные обязательства. | **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 |
| **ISA 62443-2-1:2009** 4.3.2.6.7 |
| **ISA 62443-3-3:2013** SR 6.1 |
| **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 |
| **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12 |
| **ID.SC-5:** Планирование и тестирование реагирования и восстановления проводятся с поставщиками и сторонними поставщиками. | **CIS CSC** 19, 20 |
| **COBIT 5** DSS04.04 |
| **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 |
| **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 |
| **ISO/IEC 27001:2013** A.17.1.3 |
| **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9 |

1. **Защита объектов системы.** Protected(PR)

В данном разделе представлены меры, применяемые к объектам системы, на постоянной основе и в случае возникновения чрезвычайных ситуаций.

* 1. **Identity Management, Authentication and Access Control (PR.AC):** Доступ к физическим и логическим активам и связанным с ними средствам ограничен авторизованными пользователями, процессами и устройствами и управляется в соответствии с оцененным риском несанкционированного доступа к авторизованным действиям и транзакциям.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **PR.AC-1:** Удостоверения и учетные данные выдаются, управляются, проверяются, отзываются и проверяются для авторизованных устройств, пользователей и процессов. | **CIS** **CSC** 1, 5, 15, 16 |
| **COBIT 5** DSS05.04, DSS06.03 |
| **ISA 62443-2-1:2009** 4.3.3.5.1 |
| **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 |
| **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 |
| **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 |
| **PR.AC-2:** Физический доступ к активам управляется и защищен | **COBIT 5** DSS01.04, DSS05.05 |
| **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 |
| **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 |
| **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 |
| **PR.AC-3:** Удаленный доступ управляется | **CIS CSC** 12 |
| **COBIT 5** APO13.01, DSS01.04, DSS05.03 |
| **ISA 62443-2-1:2009** 4.3.3.6.6 |
| **ISA 62443-3-3:2013** SR 1.13, SR 2.6 |
| **ISO/IEC 27001:2013** A.6.2.1,A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 |
| **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15 |
| **PR.AC-4:** Разрешения на доступ и авторизация управляются с учетом принципов наименьших привилегий и разделения обязанностей. | **CIS** **CSC** 3, 5, 12, 14, 15, 16, 18 |
| **COBIT 5** DSS05.04 |
| **ISA 62443-2-1:2009** 4.3.3.7.3 |
| **ISA 62443-3-3:2013** SR 2.1 |
| **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 |
| **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 |
| **PR.AC-5:** Целостность сети защищена (например, сегрегация сети, сегментация сети) | **CIS** **CSC** 9, 14, 15, 18 |
| **COBIT 5** DSS01.05, DSS05.02 |
| **ISA 62443-2-1:2009** 4.3.3.4 |
| **ISA 62443-3-3:2013** SR 3.1, SR 3.8 |
| **ISO/IEC 27001:2013** A.13.1.1,A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 |
| **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7 |
| **PR.AC-6:** Личности проверяются, привязываются к учетным данным и утверждаются во время взаимодействия | **CIS CSC**, 16 |
| **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 |
| **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 |
| **ISA 62443-3-3:2013** SR 1.1, SR 1.2,SR 1.4, SR 1.5, SR 1.9, SR 2.1 |
| **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 |
| **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 |
| **PR.AC-7:** Пользователи, устройства и другие активы проходят аутентификацию (например, однофакторную, многофакторную) соразмерно риску транзакции (например, рискам безопасности и конфиденциальности отдельных лиц и другим организационным рискам) | **CIS CSC** 1, 12, 15, 16 |
| **COBIT 5** DSS05.04, DSS05.10, DSS06.10 |
| **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 |
| **ISA 62443-3-3:2013** SR 1.1,SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 |
| **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 |
| **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 |

* 1. **Awareness and Training (PR.AT):** Персонал и партнеры организации проходят обучение по вопросам кибербезопасности и проходят обучение для выполнения своих обязанностей и ответственности, связанных с кибербезопасностью, в соответствии с соответствующими политиками, процедурами и соглашениями.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **PR.AT-1:** Все пользователи проинформированы и обучены | **CIS CSC** 17, 18 |
| **COBIT 5** APO07.03, BAI05.07 |
| **ISA 62443-2-1:2009** 4.3.2.4.2 |
| **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 |
| **NIST SP 800-53** **Rev. 4** AT-2, PM-13 |
| **PR.AT-2:** Привилегированные пользователи понимают свои роли и обязанности | **CIS CSC** 5, 17, 18 |
| **COBIT 5** APO07.02, DSS05.04, DSS06.03 |
| **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 |
| **ISO/IEC 27001:2013** A.6.1.1,A.7.2.2 |
| **NIST SP 800-53** **Rev. 4** AT-3, PM-13 |
| **PR.AT-3:** Сторонние заинтересованные стороны (например, поставщики, клиенты, партнеры) понимают свои роли и обязанности | **CIS** **CSC** 17 |
| **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 |
| **ISA 62443-2-1:2009** 4.3.2.4.2 |
| **ISO/IEC 27001:2013** A.6.1.1,A.7.2.1,A.7.2.2 |
| **NIST SP 800-53** **Rev. 4** PS-7, SA-9, SA-16 |
| **PR.AT-4:** Руководители высшего звена понимают свои роли и обязанности | **CIS** **CSC** 17, 19 |
| **COBIT 5** EDM01.01, APO01.02, APO07.03 |
| **ISA 62443-2-1:2009** 4.3.2.4.2 |
| **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 |
| **NIST SP 800-53** **Rev. 4** AT-3, PM-13 |
| **PR.AT-5:** Персонал по физической и кибербезопасности понимает свои роли и обязанности | **CIS** **CSC** 17 |
| **COBIT 5** APO07.03 |
| **ISA 62443-2-1:2009** 4.3.2.4.2 |
| **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 |
| **NIST SP 800-53** **Rev. 4** AT-3, IR-2, PM-13 |

* 1. **Data Security (PR.DS):** Информация и записи (данные) управляются в соответствии со стратегией управления рисками организации для защиты конфиденциальности, целостности и доступности информации.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **PR.DS-1:** Сохраненные данные защищены | **CIS** **CSC** 13, 14 |
| **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 |
| **ISA 62443-3-3:2013** SR 3.4, SR 4.1 |
| **ISO/IEC 27001:2013** A.8.2.3 |
| **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28 |
| **PR.DS-2:** Данные в пути защищены | **CIS** **CSC** 13, 14 |
| **COBIT 5** APO01.06, DSS05.02, DSS06.06 |
| **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 |
| **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 |
| **NIST SP 800-53** **Rev. 4** SC-8, SC-11, SC-12 |
| **PR.DS-3:** Активы формально управляются на протяжении всего процесса удаления, передачи и утилизации. | **CIS CSC** 1 |
| **COBIT 5** BAI09.03 |
| **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 |
| **ISA 62443-3-3:2013** SR 4.2 |
| **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 |
| **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16 |
| **PR.DS-4:** Достаточная мощность для обеспечения доступности | **CIS CSC** 1, 2, 13 |
| **COBIT 5** APO13.01, BAI04.04 |
| **ISA 62443-3-3:2013** SR 7.1, SR 7.2 |
| **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 |
| **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5 |
| **PR.DS-5:** Реализованы защиты от утечки данных. | **CIS CSC** 13 |
| **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 |
| **ISA 62443-3-3:2013** SR 5.2 |
| **ISO/IEC 27001:2013** A.6.1.2,A.7.1.1,A.7.1.2, A.7.3.1,A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 |
| **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 |
| **PR.DS-6:** Механизмы проверки целостности используются для проверки целостности программного обеспечения, микропрограмм и информации. | **CIS CSC** 2, 3 |
| **COBIT 5** APO01.06, BAI06.01, DSS06.02 |
| **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 |
| **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 |
| **NIST SP 800-53** **Rev. 4** SC-16, SI-7 |
| **PR.DS-7:** Среда разработки и тестирования отделены от производственной среды. | **CIS CSC** 18, 20 |
| **COBIT 5** BAI03.08,BAI07.04 |
| **ISO/IEC 27001:2013** A.12.1.4 |
| **NIST SP 800-53 Rev. 4** CM-2 |
| **PR.DS-8:** Механизмы проверки целостности используются для проверки целостности оборудования. | **COBIT 5** BAI03.05 |
| **ISA 62443-2-1:2009** 4.3.4.4.4 |
| **ISO/IEC 27001:2013** A.11.2.4 |
| **NIST SP 800-53 Rev. 4** SA-10, SI-7 |

* 1. **Information Protection Processes and Procedures (PR.IP):** Политики безопасности (которые определяют цель, область действия, роли, обязанности, обязательства руководства и координацию между подразделениями организации), процессы и процедуры поддерживаются и используются для управления защитой информационных систем и активов.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **PR.IP-1:** Базовая конфигурация информационных технологий / промышленных систем управления создается и поддерживается с учетом принципов безопасности (например, концепции минимальной функциональности). | **CIS** **CSC** 3, 9, 11 |
| **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 |
| **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 |
| **ISA 62443-3-3:2013** SR 7.6 |
| **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 |
| **NIST SP 800-53** **Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 |
| **PR.IP-2:** Реализован жизненный цикл разработки системы для управления системами. | **CIS** **CSC** 18 |
| **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 |
| **ISA 62443-2-1:2009** 4.3.4.3.3 |
| **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 |
| **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17 |
| **PR.IP-3:** Имеются процессы контроля изменений конфигурации | **CIS** **CSC** 3, 11 |
| **COBIT 5** BAI01.06, BAI06.01 |
| **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 |
| **ISA 62443-3-3:2013** SR 7.6 |
| **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 |
| **NIST SP 800-53** **Rev. 4** CM-3, CM-4, SA-10 |
| **PR.IP-4:** Резервное копирование информации выполняется, поддерживается и тестируется | **CIS** **CSC** 10 |
| **COBIT 5** APO13.01, DSS01.01, DSS04.07 |
| **ISA 62443-2-1:2009** 4.3.4.3.9 |
| **ISA 62443-3-3:2013** SR 7.3, SR 7.4 |
| **ISO/IEC 27001:2013** A.12.3.1,A.17.1.2, A.17.1.3, A.18.1.3 |
| **NIST SP 800-53** **Rev. 4** CP-4, CP-6, CP-9 |
| **PR.IP-5:** Соблюдаются политика и правила в отношении физической операционной среды для активов организации | **COBIT 5** DSS01.04, DSS05.05 |
| **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 |
| **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 |
| **NIST SP 800-53** **Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 |
| **PR.IP-6:** Данные уничтожаются в соответствии с политикой | **COBIT 5** BAI09.03, DSS05.06 |
| **ISA 62443-2-1:2009** 4.3.4.4.4 |
| **ISA 62443-3-3:2013** SR 4.2 |
| **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 |
| **NIST SP 800-53 Rev. 4** MP-6 |
| **PR.IP-7:** Улучшены процессы защиты | **COBIT 5** APO11.06, APO12.06, DSS04.05 |
| **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 |
| **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 |
| **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 |
| **PR.IP-8:** Разделяется эффективность технологий защиты | **COBIT 5** BAI08.04, DSS03.04 |
| **ISO/IEC 27001:2013** A.16.1.6 |
| **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4 |
| **PR.IP-9:** Планы реагирования (реагирование на инциденты и непрерывность бизнеса) и планы восстановления (восстановление после инцидентов и аварийное восстановление) существуют и управляются | **CIS** **CSC** 19 |
| **COBIT 5** APO12.06,DSS04.03 |
| **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 |
| **ISO/IEC 27001:2013** A.16.1.1,A.17.1.1, A.17.1.2, A.17.1.3 |
| **NIST SP 800-53** **Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 |
| **PR.IP-10:** Планы реагирования и восстановления проверены | **CIS** **CSC** 19, 20 |
| **COBIT 5** DSS04.04 |
| **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 |
| **ISA 62443-3-3:2013** SR 3.3 |
| **ISO/IEC 27001:2013** A.17.1.3 |
| **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14 |
| **PR.IP-11:** Кибербезопасность включена в практику управления персоналом (например, деинициализация, проверка персонала) | **CIS** **CSC** 5, 16 |
| **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 |
| **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 |
| **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 |
| **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 |
| **PR.IP-12:** План управления уязвимостями разработан и внедрен | **CIS** **CSC** 4, 18, 20 |
| **COBIT 5** BAI03.10, DSS05.01, DSS05.02 |
| **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 |
| **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2 |

* 1. **Maintenance (PR.MA):** Техническое обслуживание и ремонт компонентов производственного контроля и информационных систем выполняются в соответствии с политиками и процедурами.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **PR.MA-1:** Техническое обслуживание и ремонт активов организации выполняются и регистрируются с помощью утвержденных и контролируемых инструментов. | **COBIT 5** BAI03.10,BAI09.02,BAI09.03, DSS01.05 |
| **ISA 62443-2-1:2009** 4.3.3.3.7 |
| **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 |
| **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6 |
| **PR.MA-2:** Удаленное обслуживание активов организации утверждается, регистрируется и выполняется таким образом, чтобы предотвратить несанкционированный доступ. | **CIS** **CSC** 3, 5 |
| **COBIT 5** DSS05.04 |
| **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 |
| **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 |
| **NIST SP 800-53 Rev. 4** MA-4 |

* 1. **Protective Technology (PR.PT):** Решения технической безопасности управляются для обеспечения безопасности и отказоустойчивости систем и активов в соответствии с соответствующими политиками, процедурами и соглашениями.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **PR.PT-1:** Записи аудита / журнала определяются, документируются, внедряются и анализируются в соответствии с политикой. | **CIS CSC** 1, 3, 5, 6, 14, 15, 16 |
| **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 |
| **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 |
| **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 |
| **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 |
| **NIST SP 800-53** **Rev. 4** AU Family |
| **PR.PT-2:** Съемный носитель защищен, и его использование ограничено в соответствии с политикой | **CIS** **CSC** 8, 13 |
| **COBIT 5** APO13.01, DSS05.02, DSS05.06 |
| **ISA 62443-3-3:2013** SR 2.3 |
| **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 |
| **NIST SP 800-53** **Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 |
| **PR.PT-3:** Принцип наименьшей функциональности реализуется путем настройки систем для предоставления только необходимых возможностей. | **CIS** **CSC** 3, 11, 14 |
| **COBIT 5** DSS05.02, DSS05.05, DSS06.06 |
| **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 |
| **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 |
| **ISO/IEC 27001:2013** A.9.1.2 |
| **NIST SP 800-53 Rev. 4** AC-3, CM-7 |
| **PR.PT-4:** Сети связи и управления защищены | **CIS CSC** 8, 12, 15 |
| **COBIT 5** DSS05.02, APO13.01 |
| **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 |
| **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 |
| **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43 |
| **PR.PT-5:** Реализованы механизмы (например, отказоустойчивость, балансировка нагрузки, горячая замена) для достижения требований устойчивости в нормальных и неблагоприятных ситуациях. | **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 |
| **ISA 62443-2-1:2009** 4.3.2.5.2 |
| **ISA 62443-3-3:2013** SR 7.1, SR 7.2 |
| **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 |
| **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6 |

1. **Обнаружение угроз.**Detection(DE)

**На этапе обнаружения угроз**

* 1. **Anomalies and Events (DE.AE):** Выявляется аномальная активность и понимается возможное влияние событий.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **DE.AE-1:** Базовый план сетевых операций и ожидаемых потоков данных для пользователей и систем установлен и управляется | **CIS** **CSC** 1, 4, 6, 12, 13, 15, 16 |
| **COBIT 5** DSS03.01 |
| **ISA 62443-2-1:2009** 4.4.3.3 |
| **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 |
| **NIST SP 800-53** **Rev. 4** AC-4, CA-3, CM-2, SI-4 |
| **DE.AE-2:** Обнаруженные события анализируются для понимания целей и методов атаки. | **CIS** **CSC** 3, 6, 13, 15 |
| **COBIT 5** DSS05.07 |
| **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 |
| **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 |
| **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 |
| **NIST SP 800-53** **Rev. 4** AU-6, CA-7, IR-4, SI-4 |
| **DE.AE-3:** Данные о событиях собираются и сопоставляются из нескольких источников и датчиков. | **CIS** **CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 |
| **COBIT 5** BAI08.02 |
| **ISA 62443-3-3:2013** SR 6.1 |
| **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 |
| **NIST SP 800-53** **Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 |
| **DE.AE-4:** Влияние событий определено | **CIS** **CSC** 4, 6 |
| **COBIT 5** APO12.06, DSS03.01 |
| **ISO/IEC 27001:2013** A.16.1.4 |
| **NIST SP 800-53** **Rev. 4** CP-2, IR-4, RA-3, SI-4 |
| **DE.AE-5:** Установлены пороги предупреждения об инцидентах | **CIS** **CSC** 6, 19 |
| **COBIT 5** APO12.06, DSS03.01 |
| **ISA 62443-2-1:2009** 4.2.3.10 |
| **ISO/IEC 27001:2013** A.16.1.4 |
| **NIST SP 800-53** **Rev. 4** IR-4, IR-5, IR-8 |

* 1. **Security Continuous Monitoring (DE.CM):** Информационная система и активы отслеживаются для выявления событий кибербезопасности и проверки эффективности защитных мер.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **DE.CM-1:** Сеть отслеживается для обнаружения потенциальных событий кибербезопасности. | **CIS CSC** 1, 7, 8, 12, 13, 15, 16 |
| **COBIT 5** DSS01.03, DSS03.05,DSS05.07 |
| **ISA 62443-3-3:2013** SR 6.2 |
| **NIST SP 800-53** **Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 |
| **DE.CM-2:** Физическая среда отслеживается для обнаружения потенциальных событий кибербезопасности. | **COBIT 5** DSS01.04, DSS01.05 |
| **ISA 62443-2-1:2009** 4.3.3.3.8 |
| **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 |
| **NIST SP 800-53** **Rev. 4** CA-7, PE-3, PE-6, PE-20 |
| **DE.CM-3:** Мониторинг деятельности персонала для выявления потенциальных событий кибербезопасности | **CIS** **CSC** 5, 7, 14, 16 |
| **COBIT 5** DSS05.07 |
| **ISA 62443-3-3:2013** SR 6.2 |
| **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 |
| **NIST SP 800-53** **Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 |
| **DE.CM-4:** Обнаружен вредоносный код | **CIS CSC** 4, 7, 8, 12 |
| **COBIT 5** DSS05.01 |
| **ISA 62443-2-1:2009** 4.3.4.3.8 |
| **ISA 62443-3-3:2013** SR 3.2 |
| **ISO/IEC 27001:2013** A.12.2.1 |
| **NIST SP 800-53 Rev. 4** SI-3, SI-8 |
| **DE.CM-5:** Обнаружен неавторизованный мобильный код | **CIS** **CSC** 7, 8 |
| **COBIT 5** DSS05.01 |
| **ISA 62443-3-3:2013** SR 2.4 |
| **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 |
| **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44 |
| **DE.CM-6:** Активность внешнего поставщика услуг отслеживается для выявления потенциальных событий кибербезопасности | **COBIT 5** APO07.06, APO10.05 |
| **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 |
| **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4 |
| **DE.CM-7:** Осуществляется мониторинг неавторизованного персонала, подключений, устройств и программного обеспечения. | **CIS** **CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 |
| **COBIT 5** DSS05.02, DSS05.05 |
| **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 |
| **NIST SP 800-53** **Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 |
| **DE.CM-8:** Выполняется сканирование уязвимостей | **CIS** **CSC** 4, 20 |
| **COBIT 5** BAI03.10, DSS05.01 |
| **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 |
| **ISO/IEC 27001:2013** A.12.6.1 |
| **NIST SP 800-53** **Rev. 4** RA-5 |

* 1. **Detection Processes (DE.DP):** Процессы и процедуры обнаружения поддерживаются и тестируются, чтобы гарантировать осведомленность об аномальных событиях.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **DE.DP-1:** Роли и обязанности по обнаружению четко определены, чтобы обеспечить подотчетность | **CIS CSC** 19 |
| **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 |
| **ISA 62443-2-1:2009** 4.4.3.1 |
| **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 |
| **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14 |
| **DE.DP-2:** Действия по обнаружению соответствуют всем применимым требованиям | **COBIT 5** DSS06.01, MEA03.03, MEA03.04 |
| **ISA 62443-2-1:2009** 4.4.3.2 |
| **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 |
| **NIST SP 800-53 Rev. 4** AC-25,CA-2, CA-7, SA-18, SI-4, PM-14 |
| **DE.DP-3:** Процессы обнаружения протестированы | **COBIT 5** APO13.02, DSS05.02 |
| **ISA 62443-2-1:2009** 4.4.3.2 |
| **ISA 62443-3-3:2013** SR 3.3 |
| **ISO/IEC 27001:2013** A.14.2.8 |
| **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14 |
| **DE.DP-4:** Передается информация об обнаружении событий | **CIS** **CSC** 19 |
| **COBIT 5** APO08.04, APO12.06, DSS02.05 |
| **ISA 62443-2-1:2009** 4.3.4.5.9 |
| **ISA 62443-3-3:2013** SR 6.1 |
| **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 |
| **NIST SP 800-53** **Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4 |
| **DE.DP-5:** Процессы обнаружения постоянно улучшаются | **COBIT 5** APO11.06, APO12.06, DSS04.05 |
| **ISA 62443-2-1:2009** 4.4.3.4 |
| **ISO/IEC 27001:2013** A.16.1.6 |
| **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 |

1. **Реагирование.** Response (RS)

На этапе реагирования производится оповещение соответствующих служб о произошедшем инциденте и фиксация данных в журнале инцидентов.

* 1. **Response Planning (RS.RP):** Процессы и процедуры реагирования выполняются и поддерживаются, чтобы гарантировать реагирование на обнаруженные инциденты кибербезопасности.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **RS.RP-1:** План реагирования выполняется во время или после инцидента | **CIS CSC** 19 |
| **COBIT 5** APO12.06,BAI01.10 |
| **ISA 62443-2-1:2009** 4.3.4.5.1 |
| **ISO/IEC 27001:2013** A.16.1.5 |
| **NIST SP 800-53** **Rev. 4** CP-2, CP-10, IR-4, IR-8 |

* 1. **Communications (RS.CO):** Действия реагирования координируются с внутренними и внешними заинтересованными сторонами (например, внешняя поддержка со стороны правоохранительных органов).

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **RS.CO-1:** Персонал знает свои роли и порядок действий, когда требуется ответ | **CIS** **CSC** 19 |
| **COBIT 5** EDM03.02, APO01.02, APO12.03 |
| **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 |
| **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 |
| **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8 |
| **RS.CO-2:** Сообщается об инцидентах в соответствии с установленными критериями | **CIS** **CSC** 19 |
| **COBIT 5** DSS01.03 |
| **ISA 62443-2-1:2009** 4.3.4.5.5 |
| **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 |
| **NIST SP 800-53 Rev. 4** AU-6,IR-6, IR-8 |
| **RS.CO-3:** Информация предоставляется в соответствии с планами реагирования | **CIS** **CSC** 19 |
| **COBIT 5** DSS03.04 |
| **ISA 62443-2-1:2009** 4.3.4.5.2 |
| **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 |
| **NIST SP 800-53** **Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 |
| **RS.CO-4:** Координация с заинтересованными сторонами происходит в соответствии с планами реагирования | **CIS** **CSC** 19 |
| **COBIT 5** DSS03.04 |
| **ISA 62443-2-1:2009** 4.3.4.5.5 |
| **ISO/IEC 27001:2013** Clause 7.4 |
| **NIST SP 800-53** **Rev. 4** CP-2, IR-4, IR-8 |
| **RS.CO-5:** Добровольный обмен информацией происходит с внешними заинтересованными сторонами для достижения более широкой ситуационной осведомленности о кибербезопасности | **CIS** **CSC** 19 |
| **COBIT 5** BAI08.04 |
| **ISO/IEC 27001:2013** A.6.1.4 |
| **NIST SP 800-53 Rev. 4** SI-5, PM-15 |

* 1. **Analysis (RS.AN):** Анализ проводится для обеспечения эффективного реагирования и поддержки восстановительных работ.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **RS.AN-1:** Уведомления от систем обнаружения исследуются | **CIS** **CSC** 4, 6, 8, 19 |
| **COBIT 5** DSS02.04,DSS02.07 |
| **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 |
| **ISA 62443-3-3:2013** SR 6.1 |
| **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 |
| **NIST SP 800-53** **Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 |
| **RS.AN-2:** Последствия инцидента понятны | **COBIT 5** DSS02.02 |
| **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 |
| **ISO/IEC 27001:2013** A.16.1.4,A.16.1.6 |
| **NIST SP 800-53** **Rev. 4** CP-2, IR-4 |
| **RS.AN-3:** Криминалистика проводится | **COBIT 5** APO12.06, DSS03.02, DSS05.07 |
| **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 |
| **ISO/IEC 27001:2013** A.16.1.7 |
| **NIST SP 800-53** **Rev. 4** AU-7, IR-4 |
| **RS.AN-4:** Инциденты классифицируются в соответствии с планами реагирования | **CIS** **CSC** 19 |
| **COBIT 5** DSS02.02 |
| **ISA 62443-2-1:2009** 4.3.4.5.6 |
| **ISO/IEC 27001:2013** A.16.1.4 |
| **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8 |
| **RS.AN-5:** Установлены процессы для получения, анализа и реагирования на уязвимости, раскрытые организации из внутренних и внешних источников (например, внутреннее тестирование, бюллетени по безопасности или исследователи безопасности) | **CIS CSC** 4, 19 |
| **COBIT 5** EDM03.02, DSS05.07 |
| **NIST SP 800-53 Rev. 4** SI-5, PM-15 |

* 1. **Mitigation (RS.MI):** Выполняются действия для предотвращения распространения события, смягчения его последствий и разрешения инцидента.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **RS.MI-1:** Инциденты сдерживаются | **CIS** **CSC** 19 |
| **COBIT 5** APO12.06 |
| **ISA 62443-2-1:2009** 4.3.4.5.6 |
| **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 |
| **ISO/IEC 27001:2013** A.12.2.1,A.16.1.5 |
| **NIST SP 800-53 Rev. 4** IR-4 |
| **RS.MI-2:** Инциденты смягчаются | **CIS** **CSC** 4, 19 |
| **COBIT 5** APO12.06 |
| **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 |
| **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 |
| **NIST SP 800-53 Rev. 4** IR-4 |
| **RS.MI-3:** Вновь выявленные уязвимости устраняются или документируются как принятые риски | **CIS** **CSC** 4 |
| **COBIT 5** APO12.06 |
| **ISO/IEC 27001:2013** A.12.6.1 |
| **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5 |

* 1. **Improvements (RS.IM):** Организационные мероприятия по реагированию улучшаются за счет включения уроков, извлеченных из текущих и предыдущих мероприятий по обнаружению/реагированию.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **RS.IM-1:** В планах реагирования учтены извлеченные уроки | **COBIT 5** BAI01.13 |
| **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 |
| **ISO/IEC 27001:2013** A.16.1.6, Clause 10 |
| **NIST SP 800-53** **Rev. 4** CP-2, IR-4, IR-8 |
| **RS.IM-2:** Обновлены стратегии реагирования | **COBIT 5** BAI01.13, DSS04.08 |
| **ISO/IEC 27001:2013** A.16.1.6, Clause 10 |
| **NIST SP 800-53** **Rev. 4** CP-2, IR-4, IR-8 |

1. **Восстановление.** Recovery(RC)

**На этапе восстановления производится устранение последствий произошедшего ранее инцидента.**

* 1. **Recovery Planning (RC.RP):** Процессы и процедуры восстановления выполняются и поддерживаются для обеспечения восстановления систем или активов, затронутых инцидентами кибербезопасности.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **RC.RP-1:** План восстановления выполняется во время или после инцидента кибербезопасности | **CIS** **CSC** 10 |
| **COBIT 5** APO12.06,DSS02.05, DSS03.04 |
| **ISO/IEC 27001:2013** A.16.1.5 |
| **NIST SP 800-53** **Rev. 4** CP-10, IR-4, IR-8 |

* 1. **Improvements (RC.IM):** Планирование и процессы восстановления улучшаются за счет включения извлеченных уроков в будущую деятельность.

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **RC.IM-1:** Планы восстановления включают извлеченные уроки | **COBIT 5** APO12.06,BAI05.07, DSS04.08 |
| **ISA 62443-2-1:2009** 4.4.3.4 |
| **ISO/IEC 27001:2013** A.16.1.6, Clause 10 |
| **NIST SP 800-53** **Rev. 4** CP-2, IR-4, IR-8 |
| **RC.IM-2:** Обновлены стратегии восстановления | **COBIT 5** APO12.06,BAI07.08 |
| **ISO/IEC 27001:2013** A.16.1.6, Clause 10 |
| **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 |

* 1. **Communications (RC.CO):** Действия по восстановлению координируются с внутренними и внешними сторонами (например, координационными центрами, поставщиками интернет-услуг, владельцами атакующих систем, жертвами, другими CSIRT и поставщиками).

|  |  |
| --- | --- |
| **Подкатегории** | **Стандарты** |
| **RC.CO-1:** Связи с общественностью управляются | **COBIT 5** EDM03.02 |
| **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4 |
| **RC.CO-2:** Репутация восстанавливается после инцидента | **COBIT 5** MEA03.02 |
| **ISO/IEC 27001:2013** Clause 7.4 |
| **RC.CO-3:** Информация о мероприятиях по восстановлению доводится до внутренних и внешних заинтересованных сторон, а также руководящих и управленческих групп. | **COBIT 5** APO12.06 |
| **ISO/IEC 27001:2013** Clause 7.4 |
| **NIST SP 800-53 Rev. 4** CP-2, IR-4 |