КОНЦЕПЦИЯ СОВЕРШЕНСТВОВАНИЯ КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

(перевод)

Дополнительные материалы к докладу на конференции **«IT Security Conference 2019»**

Подготовили:
Вячеслав Аксенов, IT Security Architect, ООО «ЮГИС групп», v.aksionov@ugis.by
Наталья Насонова, доктор техн. наук, доцент, доцент кафедры Защиты информации Белорусского государственного университета информатики и радиоэлектроники, natallianasonova@gmail.com.

г. Минск, 2019

Оглавление

РЕЗЮМЕ

Национальная и экономическая безопасность любого государства зависит от надежного функционирования критически важной инфраструктуры. Системы критически важной инфраструктуры становятся все более сложными, увеличивается количество связей внутри них и между ними, что делает их более подверженным угрозам информационной безопасности, подвергая риску государственную, экономическую и общественную безопасность. Так же, как и финансовые и репутационные риски, риски информационной безопасности влияют на прибыль компании, повышая затраты и воздействуя на доходы, снижая инновационные способности организации, затрудняя приобретение и удержание клиентов.

Политика государства предусматривает повышение безопасности и устойчивости государственной критически важной инфраструктуры и поддержку электронной среды, способствующей эффективности, инновациям и экономическому успеху, одновременно содействуя безопасности, защищенности бизнеса, поддержке конфиденциальности и гражданских свобод. Добровольная Концепция Информационной безопасности является риск-ориентированной и представляет собой комплекс промышленных стандартов и передовых подходов для помощи организациям в управлении рисками информационной безопасности. Концепция, созданная при сотрудничестве правительства и частного сектора, рентабельна и использует общий язык для описания и управления рисками информационной безопасности, основываясь на потребностях бизнеса и не устанавливая дополнительных нормативных требований.

Концепция фокусируется на использовании бизнес-факторов при руководстве деятельностью по информационной безопасности, а также рассматривает риски информационной безопасности, как часть процессов управления рисками организации. Концепция состоит из трех частей: Ядро Концепции, Профиль Концепции и Уровни Реализации Концепции. Ядро Концепции – это совокупность мероприятий по информационной безопасности, их результатов и справочного материала, общих для отраслей критически важной инфраструктуры, которые образуют детальное руководство по разработке индивидуальных Профилей для организаций. Использование Профилей Концепции помогает организации привести ее деятельность по информационной безопасности в соответствие с бизнес-требованиями, толерантностью к риску и ресурсами. Уровни Реализации предоставляют организациям механизм для оценки и осознания эффективности их подхода к управлению риском информационной безопасности. Концепция также предусматривает защиту личных и гражданских свобод при проведении мероприятий по информационной безопасности в организациях критически

ООО «ЮГИС групп», Беларусь, 220030 Минск, ул. Красноармейская, 20А/1,
тел. +375 29 779 32 28 info@ugis.by

важной инфраструктуры и помогает организациям включить вопросы личных и гражданских свобод в комплексную программу информационной безопасности.

Концепция дает возможность организациям, независимо от их размера, степени риска информационной безопасности или сложности системы информационной безопасности, применять современные принципы и передовые подходы управления рисками для повышения безопасности и устойчивости критически важной инфраструктуры. Для этого в Концепции собраны стандарты, руководства и практики, эффективно действующие в промышленности в настоящее время. Отсылка к общепризнанным стандартам информационной безопасности позволяет использовать ее в качестве модели для международного сотрудничества и усиления информационной безопасности критически важной инфраструктуры.

Концепция не является универсальным подходом к управлению рисками информационной безопасности критически важной инфраструктуры. Организациям могут быть присущи свои специфичные риски – различные угрозы, уязвимости, различная толерантность к риску – и способы реализации подходов Концепции будут варьироваться. Организации сами определяют деятельность, необходимую для оказания критически важных услуг, и выделяют приоритет инвестиций для получения максимальной отдачи от вложений. В итоге Концепция нацелена на снижение и более эффективное управление рисками информационной безопасности. Концепция – живой документ и продолжает обновляться и совершенствоваться на основе обратной связи по результатам внедрения, получаемой из отраслей промышленности. Опыт, получаемый при внедрении Концепции, учитывается в последующих версиях. Это позволяет удовлетворить требованиям владельцев и операторов критически важной инфраструктуры в динамичных и сложных условиях новых угроз, рисков и решений.

Использование, развитие и взаимный обмен рекомендациями этой Концепции – это шаги к повышению информационной безопасности государственной критически важной инфраструктуры, включающие создание правил для отдельных организаций, что приводит к улучшению состояния информационной безопасности государственной критически важной инфраструктуры в целом.

1.0 ВВЕДЕНИЕ В КОНЦЕПЦИЮ

Национальная и экономическая безопасность зависят от надежного функционирования критически важной инфраструктуры. Для повышения устойчивости этой инфраструктуры необходима разработка добровольной Концепции информационной безопасности (Концепция), которая предложит приоритезированный, гибкий, воспроизводимый, результативный и экономически эффективный подход для управления рисками информационной безопасности для тех процессов, информации и систем, которые напрямую участвуют в оказании услуг критически важной инфраструктуры. Концепция, разработанная в сотрудничестве с промышленностью, содержит руководство для организаций по управлению рисками информационной безопасности.

Критически важная инфраструктура определяется как системы и ресурсы, физические или виртуальные, настолько важные для государства, что выход из строя или разрушение таких систем и ресурсов приведет к значительным негативным последствиям для национальной безопасности в экономической, социальной, экологической сферах. Из-за возрастающего давления внешних и внутренних угроз организациям, ответственным за критически важную инфраструктуру, необходим последовательный и итеративный (повторяющийся) подход для идентификации, оценки и управления рисками информационной безопасности. Этот подход необходим в независимости от размера организации, ее подверженности угрозам или сложности ее системы информационной безопасности.

Критически важная инфраструктура представлена государственными и частными владельцами и операторами и другими организациями, участвующими в безопасности национальной инфраструктуры. Организации критически важной инфраструктуры выполняют функции, которые поддерживаются информационными технологиями (ИТ) и автоматизированными системами управления технологическими процессами (АСУ ТП). Эта зависимость от технологии, связи и взаимосвязи ИТ и АСУ изменила и расширила перечень потенциальных уязвимостей и увеличила потенциальный риск для деятельности организаций. Например, АСУ и данные, получаемые при работе АСУ, все больше используются для оказания критически важных услуг и поддержки бизнес-решений, поэтому необходимо учитывать потенциальное влияние инцидента информационной безопасности на бизнес, ресурсы, экологию и безопасность организации. Для управления рисками информационной безопасности требуется четкое представление бизнес-факторов организации и среды безопасности, характерных для используемых ИТ и АСУ. Из-за специфичности рисков каждой организации,

применяемые ИТ и АСУ, инструменты и методы для достижения результатов, описанные в Концепции, будут различаться.

Учитывая роль защиты личных и гражданских свобод в повышении общественного доверия, Концепция включает методологию защиты личных и гражданских свобод при проведении деятельности по информационной безопасности организациями критически важной инфраструктуры. Во многих организациях уже имеются процессы, учитывающие конфиденциальность и гражданские свободы. Методология дополняет такие процессы и предоставляет руководство для приведения управления рисками нарушения конфиденциальности в соответствие с управлением рисками информационной безопасности организации. Интеграция конфиденциальности и информационной безопасности предоставляет организациям преимущества за счет повышения доверия клиентов, возможности более стандартизованного совместного использования информации и упрощения действий в правовом поле.

Концепция нейтральна в отношении технологий, допуская возможности наращивания и технических инноваций. Концепция основывается на существующих стандартах, руководствах и практиках и нацелена на обеспечение устойчивости провайдеров критически важной инфраструктуры. Эти глобальные стандарты, руководства и практики разрабатываются, управляются и обновляются промышленностью, а инструменты и методы, доступные для достижения результатов Концепции достаточно универсальны, учитывают глобальную природу рисков информационной безопасности и развиваются с технологическим прогрессом и бизнес-требованиями.

Использование существующих и новых стандартов обеспечивает экономию, обусловленную ростом масштабов производства, и приводит к развитию эффективных продуктов, услуг и подходов, удовлетворяющих описанным требованиям рынка. Рыночная конкуренция также способствует более быстрому проникновению и реализации этих технологий и методов.

Концепция объединяет стандарты, руководства и практики и предлагает общую классификацию и механизм для:

1) описания текущего состояния информационной безопасности организации;

2) описания искомого состояния информационной безопасности организации;

3) идентификации и приоритезации возможностей улучшения в условиях непрерывного и повторяющегося процесса;

4) оценки прогресса в достижении искомого состояния;

5) обмена информацией о рисках информационной безопасности между внутренними и внешними участниками.

Концепция дополняет и не вытесняет процесс управления рисками и программу по информационной безопасности организации. Используя свои действующие процессы управления рисками информационной безопасности, организация с помощью Концепции может определить, как их усовершенствовать и привести в соответствие с промышленными нормами и технологиями. С другой стороны, организация без существующей программы по информационной безопасности может использовать Концепцию, как исходную точку для ее создания.

Так же как Концепция не привязана к отрасли промышленности, общая классификация стандартов, руководств и практик, которую она предлагает, также не привязана к стране. Концепция может быть использована для разработки общего языка для международного сотрудничества по информационной безопасности критически важной инфраструктуры.

1.1 Общие положения Концепции

Концепция представляет собой риск-ориентированный подход для управления рисками информационной безопасности и состоит из трех частей: Ядро Концепции, Уровни Реализации Концепции и Профили Концепции. Каждый компонент Концепции усиливает связи между бизнес-факторами и деятельностью по информационной безопасности. Эти компоненты рассмотрены далее.

- *Ядро Концепции* описывает деятельность по информационной безопасности, искомые результаты и применимые ссылки на документы, которые являются общими для всех отраслей критически важной инфраструктуры. Ядро представляет промышленные стандарты, руководства и практики в форме, которая позволяет обмениваться информацией о деятельности по информационной безопасности и ее результатах между всеми уровнями организации – от управленческого до операционного. Ядро Концепции состоит из пяти согласованных и непрерывных Функций – Идентификация, Защита, Обнаружение, Реагирование, Восстановление. В комплексе эти Функции обеспечивают высокоуровневое стратегическое представление жизненного цикла управления риском информационной безопасности организации. Ядро Концепции выделяет основные Категории и Подкатегории для каждой Функции и соответствующие им Информационные Ссылки, указывающие существующие стандарты, руководства и практики для каждой Подкатегории.
- *Уровни Реализации Концепции (Уровни)* описывают отношение организации к рискам информационной безопасности и характеризуют ее процессы управления этими рисками. Степень, в которой методы

управления рисками организации соответствуют положениям Концепции (например, осведомленный о риске и угрозах, повторяющийся, адаптивный) определяет Уровень от Частичного (Уровень 1) до Гибкого (Уровень 4). Эти Уровни отражают прогресс от неформального, пассивного реагирования до динамичных риск-ориентированных подходов. В процессе выбора Уровня организация должна учитывать свою существующую деятельность по управлению рисками, угрозы, законодательные и нормативные требования, бизнес цели и миссию и организационные ограничения.

- *Профиль Концепции (Профиль)* содержит компоненты, которые организация выбрала из Категорий и Подкатегорий Концепции на основе своих бизнес-требований. Профиль представляет собой набор стандартов, руководств и практик Ядра Концепции для конкретного плана реализации. Профили могут использоваться для определения возможностей улучшения состояния информационной безопасности, путем сравнения «Текущего» Профиля (состояние на сегодняшний момент) с «Целевым» Профилем (состоянием, к которому организация стремится). Для разработки Профиля организация из всех Категорий и Подкатегорий, основываясь на бизнес-факторах и оценке рисков, определяет наиболее важные. При необходимости для учета специфичных рисков организации Категории и Подкатегории могут добавляться. Текущий Профиль затем используется для расстановки приоритетов и измерения прогресса при достижении Целевого Профиля, одновременно удовлетворяя другим бизнес-требованиям, включая рентабельность и инновационность. Профили могут использоваться для самооценки и обмена информацией внутри организации или между организациями.

1.2 Управление рисками и Концепция Информационной безопасности

Управление рисками – это непрерывный процесс идентификации, оценки и реагирования на риски. Для управления рисками организации оценивают вероятность возникновения события и оказываемое воздействие, на основе чего определяют допустимый уровень риска при оказании услуг и выражают его в толерантности к риску.

Определив толерантность к риску, организации могут расставить приоритеты в деятельности по информационной безопасности, принимая взвешенные решения по расходованию средств на информационную безопасность. Внедрение программ управления рисками позволяет организациям измерять и корректировать свои программы информационной безопасности. Организации могут выбрать различные способы обработки рисков, включая снижение риска, избежание риска, передачу риска или его принятие в

ООО «ЮГИС групп», Беларусь, 220030 Минск, ул. Красноармейская, 20А/1,
тел. +375 29 779 32 28 info@ugis.by

зависимости от потенциального воздействия на оказание критически важных услуг.

Концепция использует процессы управления рисками для взвешивания и расстановки приоритетов в принимаемых решениях по информационной безопасности. Она использует периодически повторяющуюся оценку рисков и проверку бизнес-факторов для того, чтобы помочь организациям выбрать целевые состояния информационной безопасности, отражающие требуемые результаты. Таким образом, Концепция позволяет организации динамически выбирать и напрямую совершенствовать управление рисками информационной безопасности для ИТ и АСУ.

Концепция адаптируется и обеспечивает гибкую и риск-ориентированную реализацию, которая может применяться с большим количеством процессов управления рисками информационной безопасности. Примеры процессов управления рисками информационной безопасности включают стандарты ISO 31000:2009, ISO/IEC 27005:2011 Международной организации по стандартизации (International Organization for Standardization (ISO)), Специальное Издание (Special Publication (SP)) 800-39 Национального Института Стандартизации и Технологий (National Institute of Standards and Technology (NIST)) и Руководство по Процессу управления рисками информационной безопасности энергетической отрасли.

1.3 Содержание документа Концепции

Документ Концепции содержит следующие разделы и приложения:

- Раздел 2 описывает компоненты Концепции: Ядро Концепции, Условия и Профили
- Раздел 3 приводит пример вариантов применения Концепции
- Раздел 4 описывает применение Концепции для измерения информационной безопасности
- Приложение A представляет Ядро Концепции в табличном формате: Функции, Категории, Подкатегории и Информационные Ссылки
- Приложение B содержит глоссарий избранных терминов
- Приложение C содержит перечень сокращений, использованных в документе
- Приложение D приводит развернутое описание исправлений, внесенных в версию 1.1.

2.0 ОСНОВЫ КОНЦЕПЦИИ

Концепции предлагает общий язык для описания, управления и оценки рисков информационной безопасности, внутренних и внешних. Она помогает идентифицировать и устанавливать приоритеты для мероприятий по снижению рисков информационной безопасности, а также является инструментом по приведению в соответствие политики организации, бизнеса и технологических подходов по управлению этими рисками. Она может применяться для управления рисками информационной безопасности всей организации или фокусироваться на оказании критически важных услуг внутри организации. Различные виды организаций – включая структуры, координирующие отрасль, объединения, организации – могут использовать Программу для различных целей, в том числе и создание общих Профилей.

2.1 Ядро Концепции

Ядро Концепции содержит набор мероприятий, направленных на достижение отдельных результатов по информационной безопасности и дает ссылки на примеры руководств по достижению этих результатов. Ядро Концепции не является контрольным списком мероприятий. Оно содержит ключевые результаты по информационной безопасности, определенные промышленностью, как полезные для управления рисками информационной безопасности. Ядро состоит из четырех элементов: Функций, Категорий, Подкатегорий и Информационных Ссылок, приведенных на Рисунке 1.

Функции Концепции	Идентификация	Категории	Подкатегории	Информативные ссылки
	Защита	Категории	Подкатегории	Информативные ссылки
	Обнаружение	Категории	Подкатегории	Информативные ссылки
	Реагирование	Категории	Подкатегории	Информативные ссылки
	Восстановление	Категории	Подкатегории	Информативные ссылки

Рисунок 1. Структура Ядра Концепции

Элементы Ядра Концепции функционируют следующим образом:

- Функции направлены на организацию основных мероприятий по информационной безопасности на самом высоком уровне. В Концепции выделены пять Функций: Идентификация, Защита, Обнаружение, Реагирование и Восстановление. Они помогают организации обеспечить управление рисками информационной безопасности путем организации информации, содействия принятию решений по управлению рисками, реагирования на угрозы и внесения улучшений на основе предшествующего опыта. Функции также поддерживают существующие методы управления инцидентами и позволяют демонстрировать эффект от инвестиций в информационную безопасность. Например, инвестиции в планирование и проведение учений для персонала влияют на своевременное реагирование и мероприятия по восстановлению, снижая влияние угроз на процесс оказание услуг.
- Функции делятся на Категории, содержащие группы результатов по информационной безопасности, тесно связанные с программными требованиями и конкретными мероприятиями. Примеры Категорий – «Управление ресурсами», «Контроль ресурсов» и «Процедуры обнаружения».
- В Категориях выделяются отдельные результаты технической и/или управленческой деятельности, образуя Подкатегории. Они содержат совокупность мероприятий, направленных на достижение результатов в каждой Категории. К примерам Подкатегорий относятся: «Внешние информационные системы внесены в перечень», «Данные в местах хранения защищены» и «Уведомления систем обнаружения обработаны».
- Информационные ссылки представляют собой отдельные наборы стандартов, руководств и практик, общих для отраслей критически важной инфраструктуры и описывающих способы реализации мероприятий каждой Подкатегории. Информационные ссылки, приведенные в Ядре Концепции, пояснительные и не исчерпывающие. Они основываются на межотраслевых руководствах, наиболее часто использованных в процессе разработке Концепции.

Ниже описаны пять Функций Ядра Концепции. Эти Функции не являются последовательными действиями и не предназначены для достижения статичного искомого окончательного состояния. Наоборот, Функции могут выполняться одновременно и непрерывно, чтобы создать операционную культуру, учитывающую динамические риски информационной безопасности. В Приложении А приведен полный состав Ядра Концепции.

- **Идентификация** – разработка подхода организации к управлению рисками информационной безопасности для систем, ресурсов, данных и инфраструктуры.
  Мероприятия, предусмотренные Функцией Идентификации, – основа для эффективного использования Концепции. Понимание условий бизнеса, ресурсов, поддерживающих критические функции, и связанных с ними рисков информационной безопасности заставляет организацию сфокусировать и приоритезировать свои усилия согласно ее стратегии управления риском и бизнес-требованиям. Примерами итоговых Категорий в этой Функции являются: Управление Ресурсами, Бизнес Окружение, Руководство (организацией), Оценка Риска и Стратегия Управления Риском.
- **Защита** – разработка и реализация соответствующих мер безопасности для обеспечения оказания услуг критически важной инфраструктурой.

Функция Защита способствует ограничению или сдерживанию влияния потенциального события информационной безопасности. Примерами итоговых Категорий в этой Функции являются Контроль Ресурсов, Повышение Осведомленности и Тренинги, Безопасность Данных, Процессы и Процедуры Защиты Информации, Эксплуатация, Защитная Технология.

- **Обнаружение** – разработка и реализация соответствующих мероприятий для идентификации возникновения события информационной безопасности.

Функция Обнаружение способствует своевременному обнаружению событий информационной безопасности. Примерами итоговых Категорий в этой Функции являются: Аномалии и События, Непрерывный Мониторинг Безопасности и Процессы Обнаружения.

- **Реагирование** – разработка и реализация соответствующих мероприятий для выполнения действий, относящихся к обнаруженному событию информационной безопасности.

Функция Реагирование способствует ослаблению воздействия потенциального события информационной безопасности. Примерами итоговых Категорий в этой Функции являются: Планирование Деятельности по Реагированию, Коммуникации, Анализ, Подавление и Усовершенствование.

- **Восстановление** – разработка и реализация соответствующих мероприятий по применению планов устойчивости и восстановлению характеристик или деятельности, нарушенных в результате события информационной безопасности.

Функция Восстановление способствует своевременному восстановлению к нормальной работе для снижения воздействия события информационной

безопасности. Примерами итоговых Категорий в этой Функции являются: Планирование Деятельности по Восстановлению, Усовершенствование и Коммуникации.

2.2 Уровни Реализации Концепции

Уровни Реализации Концепции (Уровни) описывают отношение организации к рискам информационной безопасности и характеризуют ее процессы управления этими рисками. Уровни изменяются от Частичного (Уровень 1) до Гибкого (Уровень 4) и отражают комплексность деятельности по управлению рисками информационной безопасности, а также насколько управление рисками информационной безопасности связано с бизнес-требованиями и интегрировано в общие практики управления рисками организации. Сфера управления рисками включает множество аспектов информационной безопасности, включая степень интеграции конфиденциальности и гражданских свобод в управление рисками информационной безопасности организации и реагирование на потенциальный риск.

Процесс выбора Уровня учитывает существующие в организации практики по управлению рисками информационной безопасности, среду угроз, законодательные и нормативные требования, технологии совместного использования информации, бизнес задачи и миссию, требования по управлению рисками цепи поставок и организационные ограничения. Организациям следует определить искомый Уровень так, чтобы он удовлетворял организационным целям, был практически реализуемым и снижал риск информационной безопасности критически важных ресурсов и активов до уровней, приемлемых для организации. Кроме этого, следует учитывать требования регулирующих государственных органов, существующие модели зрелости или другие источники.

Хотя предполагается, что организациям, отнесенным к Уровню 1 (Частичный), следует стремиться к соответствию Уровню 2 и выше, Уровни не представляют собой уровни зрелости. Прогресс к более высоким Уровням необходим, если такое изменение позволит снизить риск информационной безопасности и будет экономически оправданным. Успешная реализация Концепции основывается на достижении результатов, описанных в Целевом Профиле организации, а на не определении Уровня. Хотя выбор Уровня и его присвоение влияет на Профили Концепции. Распределение риска, выраженное в искомом Уровне, должно оказывать влияние на расстановку приоритетов в Целевом Профиле. Аналогично, состояние организации, описанное в выбранном Уровне, связано с соответствующими положениями в оцениваемом Профиле, а также дает информацию о реальном прогрессе по оценке недостатков состояния информационной безопасности организации.

Описание Уровней:

Уровень 1: Частичный

- *Процесс управления риском* – правила по управлению рисками информационной безопасности организации не формализованы, управление риском происходит ситуативно и иногда пассивно. Приоритеты в мероприятиях по информационной безопасности могут быть напрямую не обусловлены целями рисков организации, угрозами или бизнес-требованиями и миссией.
- *Интегрированная Программа Управления Риском* – ограниченная осведомленность о риске информационной безопасности на организационном уровне. Организация реализует управление риском информационной безопасности нерегулярно, время от времени, на основе опыта или информации, получаемой из внешних источников. Организация может не иметь процессов, которые позволяют совместно использовать информацию об информационной безопасности внутри организации.
- *Внешнее участие* – организация может не иметь действующих процессов для участия в координации или сотрудничестве с другими организациями.
- *Управление риском цепи поставок* – организация может не понимать полностью смысла рисков цепи поставок или не иметь действующих процессов для идентификации, оценки и снижения рисков цепи поставок.

Уровень 2: Риск-ориентированный

- *Процесс управления риском* – правила по управлению рисками одобрены руководством организации, но не приняты в качестве всеобщей политики всей организации. Приоритеты в мероприятиях по информационной безопасности напрямую обусловлены целями рисков организации, угрозами или бизнес-требованиями и миссией.
- *Интегрированная Программа Управления Риском* – присутствует осведомленность о риске информационной безопасности на организационном уровне, но отсутствует укоренившийся и общий организационный подход к управлению рисками информационной безопасности. Информация об информационной безопасности распространяется в организации по неформальным каналам. Информационная безопасность может учитываться в бизнес-задачах и миссии на некоторых уровнях организации, но не на всех.
- *Внешнее участие* – организация осознает свое место в структуре отрасли, но не формализовала свои возможности по взаимодействию и совместному распределению информации с внешними организациями.

- *Управление риском цепи поставок* – организация понимает риски цепи поставок, связанных с продуктами и услугами, которые обслуживают производственную функцию организации или используются в продуктах или услугах организации. Организация не имеет формализованных возможностей по управлению рисками цепи поставок изнутри или со своими поставщиками и партнерами и производит эту деятельность непоследовательно.

Уровень 3: Стабильный

- *Процесс управления риском* – правила по управлению рисками официально утверждены руководством организации и закреплены в политике. Правила по информационной безопасности периодически обновляются, основываясь на применении процессов управления риском к изменениям в бизнес-требованиях или миссии и изменяющейся среде угроз и технологий.
- *Интегрированная Программа Управления Риском* – присутствует общий организационный подход к управлению рисками информационной безопасности. Риск-ориентированные политики, процессы и процедуры определены, корректно реализованы и проверены. При изменении риска применяются согласованные методы для эффективного реагирования. Персонал обладает знаниями и навыками для выполнения назначенных им ролей и обязанностей. Организация непрерывно и тщательно производит мониторинг рисков информационной безопасности для ресурсов организации. Руководители верхнего звена по информационной безопасности и не по информационной безопасности периодически обсуждают риск информационной безопасности. Руководители верхнего звена обеспечивают учет информационной безопасности на всех производственных линиях организации.
- *Внешнее участие* – организация знает свои взаимосвязи и партнеров и получает от них информацию, которая делает возможным сотрудничество и принятие риск-ориентированных управленческих решений в ответ на события.
- *Управление риском цепи поставок* – общий организационный подход к управлению рисками цепи поставок устанавливается в политиках, процессах и процедурах по управлению рисками организации. Он может включать руководящую структуру (например, Совет по Риску), которая обеспечивает баланс рисков цепи поставок с другими рисками организации. Политики, процессы и процедуры реализованы согласованно, корректно и непрерывно подвергаются мониторингу и пересмотру. Персонал обладает знаниями и навыками для выполнения

назначенных им обязанностей по управлению риском цепи поставок. У организации есть формальные действующие соглашения по передаче базовых требований ее поставщикам и партнерам.

Уровень 4: Гибкий

- *Процесс управления риском* – организация адаптирует свои правила по информационной безопасности, основываясь на полученном опыте и прогнозных показателях, полученных из предшествующей и текущей деятельности по информационной безопасности. Используя процесс непрерывного совершенствования, включающий современные технологии и практики информационной безопасности, организации активно адаптируются к изменяющимся условиям информационной безопасности и своевременно реагируют на эволюционирующие и сложные угрозы.
- *Интегрированная Программа Управления Риском* – присутствует общий организационный подход к управлению рисками информационной безопасности, использующий риск-ориентированные политики, процессы и процедуры для реагирования на потенциальные события информационной безопасности. Взаимосвязь между риском информационной безопасности и бизнес-задачами и миссией четко ясна и учитывается при принятии решений. Руководители высшего звена производят мониторинг риска информационной безопасности так же, как и финансовых и другие рисков организации. Бюджет организации учитывает существующие и прогнозные условия рисков и будущие потребности, связанные с рисками. Подразделения реализуют позицию руководства и анализируют риски системного уровня в контексте потребностей и толерантности к рискам организации. Управление риском информационной безопасности – часть организационной культуры и осуществляется, исходя из данных о предшествующей деятельности, информации, полученной из других источников, и непрерывного мониторинга деятельности в системах и сетях организации. Риск информационной безопасности четко оговаривается и осознается во всех уровнях организации. Организация может быстро и эффективно просчитать изменения в бизнес-задачах и миссии в условиях угроз и технологий, в зависимости от того, как риск рассматривается и обрабатывается.
- *Внешнее участие* – организация управляет риском и активно распространяет информацию партнерам, чтобы обеспечить распространение и потребление точной и актуальной информации до возникновения события информационной безопасности.

- *Управление риском цепи поставок* – организация может быстро и эффективно просчитать возникающие риски цепи поставок, используя информацию в реальном времени и близко к реальному времени, и обменяться информацией об управлении риском цепи поставок со своими внешними поставщиками и партнерами, а также внутри организации в соответствующих видах деятельности и на всех уровнях организации. Организация обменивается информацией упреждающе и использует формальные (например, соглашения) и неформальные механизмы для развития и удержания сильных взаимосвязей со своими поставщиками, партнерами и индивидуальными потребителями и организациями.

2.3 Профиль Концепции

Профиль Концепции (Профиль) представляет собой выборку Функций, Категорий и Подкатегорий, произведенную в соответствии с бизнес-требованиями, толерантностью к риску и ресурсами организации. Профиль помогает организации создать план по снижению риска информационной безопасности, согласующийся с организационными и отраслевыми целями, учитывающий нормативные и законодательные требования и лучшие практики промышленности, а также отражающий приоритеты управления риском. Организации могут иметь множество Профилей, разработанных в соответствии с отдельными компонентами и направленных на удовлетворение их индивидуальных требований.

Профили Концепции можно использовать для описания текущего состояния или искомого целевого состояния отдельных мероприятий по информационной безопасности. Текущий Профиль отображает результаты по информационной безопасности, которые достигнуты на текущий момент. Целевой профиль содержит результаты, которые требуется получить для достижения искомых целей управления рисками информационной безопасности. Профили учитывают бизнес-требования и помогают коммуникации риска внутри и между организациями. Этот вариант Концепции не устанавливает шаблоны Профилей, допуская гибкость реализации.

Сравнение Профилей (например, Текущего и Целевого Профилей) может выявить недостатки, которые необходимо исправить для достижения целей управления рисками информационной безопасности. План мероприятий для исправления этих недостатков может быть включен в план действий, упомянутый выше. Приоритезация исправления недостатков производится, исходя из бизнес-требований организации и процессов управления риском. Риск-ориентированный подход дает возможность организации оценивать

ресурсы (например, кадровое обеспечение, финансирование), необходимые для достижения целей информационной безопасности рентабельным и приоритетным способом.

2.4 Координация реализации Концепции

На рисунке 2 показан общий поток информации и решений на следующих уровнях внутри организации:

- Руководство
- Бизнес/Процессы
- Реализация/Производственные процессы

Руководство организации доводит приоритеты миссии, доступные ресурсы и общую толерантность к риску до уровня Бизнеса/Процессов. Уровень Бизнеса/Процессов использует эту информацию, как входные данные для процесса управления рисками и затем сотрудничает с уровнем Реализации/Производственных процессов для разъяснения бизнес-требований и создания Профиля. Уровень Реализации/Производственных процессов уведомляет о ходе реализации Профиля уровень Бизнеса/Процессов, который использует эту информацию для оценки воздействия. Руководители уровня Бизнеса/Процессов отчитываются о результатах оценки воздействия уровню Руководства организации, предоставляя информацию общему для организации процессу управления риском и уровню Реализации/Производственных процессов для уведомления о влиянии на бизнес.

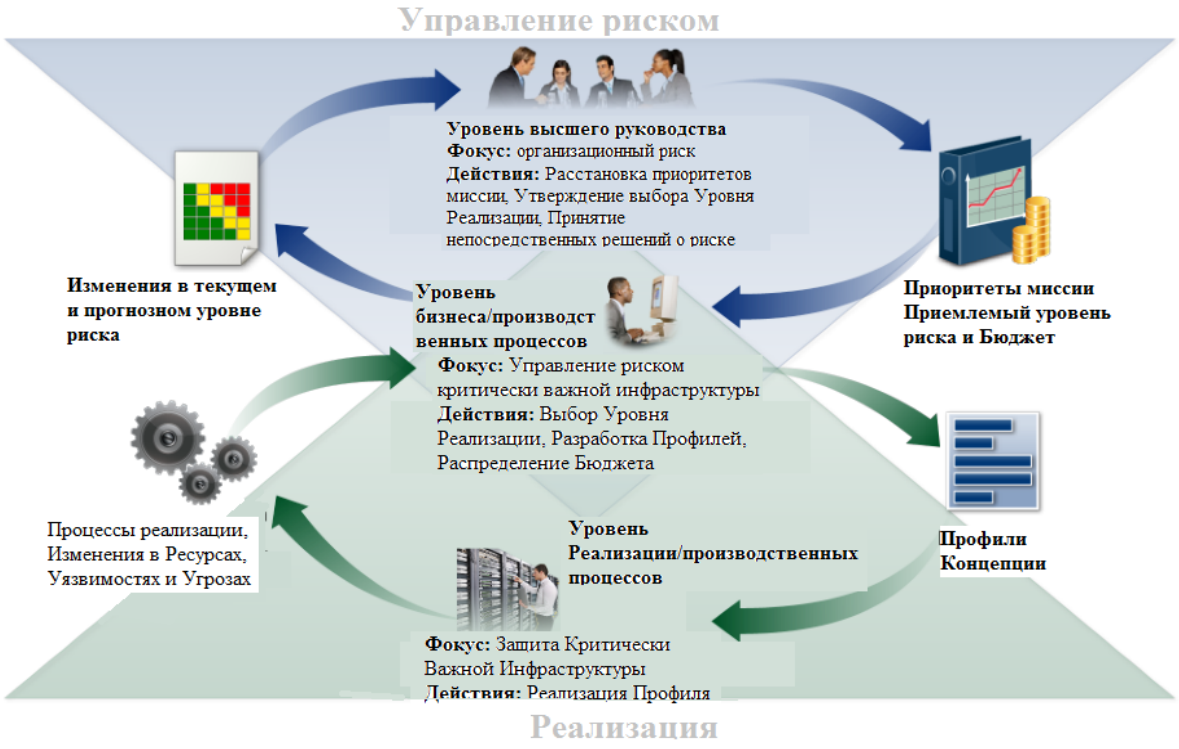

Рисунок 2. Схема потоков информации и решений в Организации

3.0 ПРИМЕНЕНИЕ КОНЦЕПЦИИ

Организация может встроить Концепцию в свой системный процесс для идентификации, оценки и управления риском информационной безопасности. Концепция не обязательно должна заместить существующие процессы; организация может использовать свои действующие процессы и сравнивать их с положениями Концепции для определения недостатков в своем подходе к риску информационной безопасности и разработки плана мероприятий по его улучшению. Используя Концепцию, как инструмент по управлению рисками информационной безопасности, организация может определить мероприятия, которые являются наиболее важными для оказания критически важных услуг, и расставить приоритеты в затратах для максимизации отдачи от инвестиций.

Концепция дополняет существующие в организации производственные процессы и процессы информационной безопасности. Она может служить основой для новой программы информационной безопасности или механизмом усовершенствования существующей программы. Используя средства Концепции, можно описать требования по информационной безопасности для бизнес-партнеров и клиентов и обнаружить пробелы в деятельности организации по информационной безопасности. Концепция также содержит набор основных положений и процессов по защите частной жизни и гражданских свобод в рамках программы по информационной безопасности.

Концепция может применяться на всех этапах жизненного цикла системы – проектирования, создания, развертывания, эксплуатации и списания. На этапе проектирования необходимо учитывать требования по информационной безопасности, как часть комплексного процесса разработки. Важным пунктом этапа проектирования является проверка соответствия технических требований к системе информационной безопасности положениям Профиля Концепции. Приоритетные результаты информационной безопасности, приведенные в Профиле, должны быть достигнуты в ходе: а) разработки системы в течение фазы создания или б) приобретения или аутсорсинга системы в течение фазы закупки. На этапе развертывания системы характеристики ее информационной безопасности должны оцениваться для проверки примененной структуры. Мероприятия по информационной безопасности, приведенные в Концепции, затем служат основой для эксплуатации системы, включая периодическую переоценку для проверки того, что требования по информационной безопасности все еще выполняются. Сложные зависимости между системами приводят к тому, что вопросы информационной безопасности должны быть внимательно изучены при списании одной или более систем.

Следующие разделы описывают различные способы применения Концепции.

3.1 Общая оценка мероприятий по информационной безопасности

Концепция может использоваться для сравнения действующих в организации мероприятий по информационной безопасности с теми, которые определены в Ядре Концепции. При создании Текущего Профиля организации могут оценить степень достижения ими результатов, описанных в Категориях и Подкатегориях Ядра, приведенных в пяти высокоуровневых Функциях: Идентификация, Защита, Обнаружение, Реагирование и Восстановление. Организация может обнаружить, что она уже достигла искомых результатов, таким образом управляя информационной безопасностью с известным риском, и напротив, обнаружить области, требующие улучшения. На основе этой информации организация разрабатывает план действий по усилению существующих мероприятий по информационной безопасности и снижению риска информационной безопасности. Организация также может обнаружить, что вкладывает чрезмерные инвестиции для достижения отдельных результатов и переустановить приоритеты ресурсов для усиления других мероприятий по информационной безопасности.

Предложенные пять высокоуровневых Функций позволяют четко выделить для высшего руководства организации и других участников основы риска информационной безопасности, оценить, как управляются идентифицированные риски и насколько их организация соответствует существующим стандартам, руководствам и практикам информационной безопасности. Концепция может также помочь организации ответить на фундаментальные вопросы, включая «на каком уровне мы находимся?». В результате организация может более осознанно усиливать свою деятельность по информационной безопасности там и тогда, когда нужно.

3.2 Создание или Улучшение Программы по Информационной Безопасности

Следующие этапы иллюстрируют, как организация может использовать Концепцию для создания новой программы по информационной безопасности или улучшения существующей. Эти этапы следует повторять по необходимости для непрерывного улучшения информационной безопасности.

Этап 1: Устанавливай приоритеты и определяй область действия. Организация идентифицирует свои бизнес-задачи и высокоуровневые приоритеты для принятия стратегических решений по реализации информационной безопасности и определяет, какие системы и ресурсы обеспечивают работу выбранных производственных линий или процессов. Концепция может быть адаптирована для обеспечения работы различных производственных линий или процессов в организации, подчиняющихся

различным бизнес-требованиям и связанных с различной толерантностью к риску. Уровень Реализации можно использовать для выражения различных показателей толерантности к риску.

Этап 2: Настройка. Когда определены производственные линии или процессы, которые входят в область применения программы по информационной безопасности, организация идентифицирует относящиеся к ним системы и ресурсы, законодательные требования и общий подход к риску. Затем проводится идентификация угроз и уязвимостей, применимых к этим системам и ресурсам.

Этап 3: Создание Текущего Профиля. Организация разрабатывает Текущий Профиль, указывая достигнутые результаты Категорий и Подкатегорий из Ядра Концепции. Если результат достигнут частично, это должно быть отмечено, чтобы учесть на последующих этапах.

Этап 4: Проведение Оценки Риска. Эта оценка может управляться общим организационным процессом управления риском или предшествующей деятельностью по оценке риска. Организация анализирует производственную среду для определения вероятности событий информационной безопасности и влияния, которое событие может оказать на организацию. Важно, чтобы организации идентифицировали появляющиеся риски и использовали информацию о угрозах информационной безопасности из внешних и внутренних источников для более четкого определения вероятности и влияния событий информационной безопасности.

Этап 5: Создание Целевого Профиля. Организация разрабатывает Целевой Профиль, содержащий Категории и Подкатегории Ядра, описывающие искомые результаты информационной безопасности. Организации также могут выработать собственные дополнительные Категории и Подкатегории для учета своих специфичных рисков. При создании Целевого Профиля может также учитываться влияние и требования внешних заинтересованных сторон, таких как отраслевые организации, клиенты и бизнес-партнеры. При использовании Профиля совместно с Уровнем Реализации характеристики Уровня должны отражаться в искомых результатах информационной безопасности.

Этап 6: Определение, Анализ и Приоритезация Недостатков. Организация сравнивает Текущий Профиль с Целевым Профилем для выявления недостатков. Затем разрабатывается приоритезированный план действий для обработки этих недостатков, привязанный к факторам бизнеса, анализу рентабельности и осознанию риска, для достижения результатов, содержащихся в Целевом Профиле. Организация определяет ресурсы, необходимые для устранения недостатков. Такое использование Профилей дает возможность организации принимать взвешенные решения по

мероприятиям по информационной безопасности, обеспечивать управление рисками и внедрять рентабельные, целевые улучшения.

Шаг 7: Реализация плана действий. Организация определяет, требуется ли и какие действия предпринять относительно недостатков, выявленных на предыдущем этапе. Затем осуществляется мониторинг действующих правил по информационной безопасности на предмет соответствия Целевому Профилю. Концепция содержит примеры Информационных ссылок, относящихся к Категориям и Подкатегориям, из которых организации могут выбрать наиболее подходящие для них стандарты, руководства и практики.

Этапы при необходимости могут повторяться для непрерывной оценки и улучшения своей информационной безопасности. Например, можно предположить, что более частое повторение этапа Настройки улучшает качество оценки риска. Таким образом, организации могут отслеживать прогресс через повторяющиеся обновления Текущего Профиля, в последующем сравнивая Текущий Профиль с Целевым Профилем. Этот процесс можно также использовать для приведения в соответствие своей программы по информационной безопасности с искомым Уровнем Реализации Концепции.

3.3 Обмен информацией о требованиях по Информационной Безопасности с Заинтересованными сторонами

Концепция предоставляет общий язык для обмена информацией о требованиях между независимыми заинтересованными сторонами, ответственными за оказание важнейших услуг критически важной инфраструктуры. Например:

- Организация может использовать Целевой Профиль для описания требований по управлению рисками информационной безопасности, предназначенных для внешнего поставщика услуг (например, услуг облака, в которое экспортируются данные).
- Организация может описывать состояние своей информационной безопасности, используя Текущий Профиль, для отчета о результатах или сравнения с требованиями.
- Владелец/оператор критически важной инфраструктуры, определивший внешнего партнера, от которого эта инфраструктура зависит, может использовать Целевой Профиль для передачи требуемых Категорий и Подкатегорий.
- Отрасль критически важной инфраструктуры может создать Целевой Профиль, который могут использовать входящие в нее организации как

основной базовый Профиль для создания своих специализированных Целевых Профилей. Кроме того, Уровни Реализации позволяют организации понять, как они встроены в общую систему информационной безопасности отрасли. Организации могут лучше управлять риском информационной безопасности, относящимся к заинтересованным сторонам, оценивая их положение как в критически важной инфраструктуре, так и в общей цифровой экономике.

Деятельность по обмену информацией между заинтересованными сторонами и проверке требований по информационной безопасности является одним из компонентов управления рисками цепи поставок. Первичной ее целью является идентификация, оценка и подавление «продуктов и услуг, которые могут содержать потенциально вредоносную функциональность, являются поддельными или уязвимыми из-за некачественного проектирования и изготовления внутри цепи поставок». Деятельность по управлению рисками цепи поставок может включать:

- Определение требований по информационной безопасности для поставщиков и партнеров по информационным технологиям (ИТ) и производственным технологиям (ПТ).
- Установка требований по информационной безопасности через формальные соглашения (например, контракты).
- Обмен информацией с поставщиками и партнерами о том, как эти требования по информационной безопасности будут проверяться и подтверждаться.
- Проверка того, как удовлетворяются требования по информационной безопасности в разнообразных оценочных методологиях.
- Управление перечисленной деятельностью.

Как показано на Рисунке 3, управление рисками цепи поставок охватывает поставщиков и потребителей ИТ и ПТ, а также других партнеров. Эти связи подчеркивают важную роль управления рисками цепи поставок в реагировании на риск информационной безопасности в критически важной инфраструктуре и цифровой экономике. Они должны быть идентифицированы и отнесены к функциям защиты и обнаружения организации, так же как протоколы реагирования и восстановления.

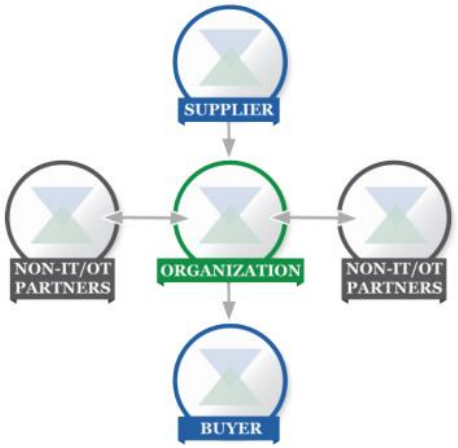

Рисунок 3. Взаимосвязи цепи поставок

К Потребителям относятся люди или организации, потребляющие данный продукт или услугу от организации. Поставщики включают провайдеров продуктов и услуг, используемых для внутренних потребностей организации (например, ИТ-инфраструктуры) или интегрируемых в продукты или услуги, поставляемые Потребителю. Партнеры, не связанные с ИТ и ПТ, имеют доступ, или имеется возможность такого доступа, к состоянию безопасности организации.

Как при помощи индивидуальных Подкатегорий Ядра, так и общих положений Профиля, Концепция предлагает организациями и их партнерам метод обеспечения соответствия нового продукта или услуги приоритетным требованиям (результатам) безопасности. После выбора результатов, относящихся к среде (передача персональных данных (ПД), оказание критически важных услуг, услуги проверки данных, интеграция продукта или услуги и т.д.), организация может затем оценивать партнеров по этим критериям. Например, при приобретении некоторой системы, которая предназначена для мониторинга производственных технологий, доступность может быть специфически важной целью, поэтому потребует выбора Подкатегории (ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5 и т.д.).

3.4 Принятие Решений о Приобретении

Поскольку Целевой Профиль Концепции представляет собой приоритезированный перечень требований по информационной безопасности организации, Целевые Профили могут использоваться для обоснования решений о приобретении продуктов и услуг. Эти операции отличаются от управления рисками цепи поставок (раздел 3.3) тем, что иногда невозможно предъявить набор требований по информационной безопасности поставщику. Вместо этого стоит вопрос выбора наилучшего

варианта по приобретению, оптимального выбранного из множества поставщиков, которым выдан предопределенный список требований по информационной безопасности. Зачастую это означает анализ компромиссных решений. В результате продукт или услуга обычно приобретается с известными несоответствиями Целевому Профилю. Когда продукт или услуга приобретены, Профиль также может быть использован для отслеживания остаточного риска информационной безопасности. Например, если приобретенные услуга или продукт не удовлетворяют всем задачам, указанным в Целевом Профиле, организация может включить этот остаточный риск информационной безопасности в общее управление рисками более крупной среды, регулируя остаточный риск управленческими действиями. Профиль также предоставляет способ гарантировать, что продукт удовлетворяет результатам по информационной безопасности в ходе периодических проверок и применения тестирующих механизмов.

3.5 Определение Применимости Новых или Пересмотренных Информационных Ссылок

С помощью Концепции можно определять применимость новых или пересмотренных стандартов, руководств или практик в качестве дополнительных Информационных Ссылок, направленных на то, чтобы помочь организации реагировать на появляющиеся потребности. Организация, реализовывая какую-либо Подкатегорию или разрабатывая новую, может обнаружить, что существует небольшое количество Информационных Ссылок или они вообще отсутствуют, для данной деятельности. Организация может сотрудничать с ведущими технологическими предприятиями и/или органами по стандартизации для проектирования, разработки и координации стандартов, руководств или практик.

3.6 Методология защиты Частной Жизни и Гражданских Свобод

Этот раздел описывает методологию, посвященную вопросам защиты конфиденциальности частной жизни и гражданских свобод, которые могут возникнуть в ходе деятельности по информационной безопасности. Эта методология представляет собой общий набор положений и процессов, поскольку особенности защиты частной жизни и гражданских свобод могут варьироваться для разных отраслей и для разных периодов времени. Организации могут применять эти положения и процессы с разнообразными вариантами технической реализации. При этом не вся деятельность программы по информационной безопасности касается этих положений. Согласно разделу 3.4, для поддержки более сложных технических реализаций

может потребоваться разработка стандартов, руководств и дополнительных подходов по технической защите информации.

Конфиденциальность и информационная безопасность сильно взаимосвязаны. Хорошо известно, что информационная безопасность играет важную роль в защите частной жизни, например, относительно ресурсов, содержащих персональные данные. Как бы там ни было, деятельность организации по защите информации также может создавать риск для конфиденциальности и гражданских свобод, когда персональные данные используются, собираются, обрабатываются, сохраняются или раскрываются в связи с деятельностью организации по защите информации. Примеры видов деятельности, которые затрагивают положения о частной жизни или гражданских свободах, включают: деятельность по защите информации, которая приводит к избыточному сбору или избыточному хранению персональных данных; раскрытие или использование персональных данных, не связанное с деятельностью по информационной безопасности; деятельность по информационной безопасности, приводящая к отказу в обслуживании или другим похожим потенциально отрицательным воздействиям, включая некоторые виды обнаружения или мониторинга инцидентов, которые могут повлиять на свободу выражения или собраний.

Правительство и служащие правительства несут прямую ответственность по защите гражданских свобод, вытекающую из деятельности по информационной безопасности. Как указано в нижеприведенной методологии, правительство и госслужащие, владеющие или эксплуатирующие критически важную инфраструктуру должны иметь действующие процессы, обеспечивающие соответствие деятельности по информационной безопасности и применимых законов о защите частной жизни, нормативными требованиями и положениями Конституции.

Для учета вопросов конфиденциальности в допустимых случаях в программу по информационной безопасности можно включить следующие принципы защиты частной жизни: минимизация данных для сбора, раскрытия, хранения персональных данных, относящихся к инциденту информационной безопасности; использование ограничений вне деятельности по информационной безопасности по отношению к любой информации, собранной специально для деятельности по информационной безопасности; прозрачность для определенных видов деятельности по информационной безопасности; индивидуальное разрешение и компенсация за отрицательные последствия, возникающие из использования персональных данных в деятельности по информационной безопасности; качество, целостность и безопасность данных; отслеживаемость и контролируемость.

Следующие процессы и мероприятия можно рассматривать, как средства обработки вышеупомянутых вопросов защиты частной жизни и гражданских свобод:

Руководство риском информационной безопасности

- Оценка организацией риска информационной безопасности и потенциальных реакций на риск учитывает вопросы защиты частной жизни
- Лица, обязанности которых связаны с защитой конфиденциальности, относящейся к защите информации, отчитываются перед соответствующим руководителями и прошли соответствующее обучение
- Имеется действующий процесс для поддержки соответствия деятельности по информационной безопасности применимым законам, нормам и положениям Конституции о защите частной жизни
- Имеется действующий процесс оценки реализации следующих организационных мер и средств управления

Подходы к идентификации и авторизации лиц для доступа к системам и ресурсам организации

- Идентифицированы и рассмотрены вопросы защиты частной жизни в мерах по контролю доступа, включающих сбор, раскрытие или использование персональных данных

Меры по повышению осведомленности и обучению

- Соответствующая информация из организационных политик по защите частной жизни включена в деятельность по обучению работников по информационной безопасности и повышению осведомленности
- Провайдеры услуг, оказывающие услуги, связанные с информационной безопасностью для организаций, уведомлены о применимых политиках защиты частной жизни в организации

Обнаружение аномальной активности и мониторинг систем и ресурсов

- Имеется действующий процесс для проведения проверки защиты частной жизни при обнаружении аномальной активности и мониторинге информационной безопасности

Деятельность по реагированию, включая обмен информацией или другие мероприятия по снижению рисков

- Имеется действующий процесс для оценки и учета, когда, как и в каком объеме персональные данные передаются за пределы организации,

который является частью мероприятий по совместному использованию информации по информационной безопасности

- Имеется действующий процесс для проверки, учитывается ли защита конфиденциальности при проведении мероприятий по снижению рисков информационной безопасности

3.7 Применение в государственных организациях

Чтобы удовлетворять требованиям по безопасности, закрепленным в нормативных и законодательных документах, необходим государственный регулятор для контроля информационной безопасности государственных информационных систем, включая системы, являющиеся частью критически важной инфраструктуры. Концепция информационной безопасности дополняет существующие государственные подходы к управлению рисками. Государственные органы могут использовать Концепцию, как ценное дополнение, используя:

- Уровни Реализации для определения предрасположенности к риску
- Ядро для организации и обмену информацией о принципах, мероприятиях и результатах деятельности по информационной безопасности
- Профили для обоснования выбора приоритетов при принятии решений
- Семиэтапный Процесс для организации деятельности по оценке и коррекции.

Государственные организации также могут использовать понятия Ядра Концепции для проведения четкого и эффективного диалога по информационной безопасности на высшем уровне между государственными и негосударственными партнерами.

4.0 ИЗМЕРЕНИЕ И ДЕМОНСТРАЦИЯ РЕЗУЛЬТАТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Измерения в Концепции являются основой для сильных доверительных связей, как внутри, так и за пределами организации. Измерение внутренних состояний и тенденций во времени, используя внешний аудит и оценку соответствия, позволяет организации определять и передавать важную информацию о риске подчиненным организациям, партнерам, клиентам.

В комбинации с Информационными ссылками Концепцию можно использовать как основу для комплексных измерений. Ключевыми терминами при проведении измерений в соответствии с Концепцией являются «Метрики» и «Показатели». Метрики используются для «облегчения

принятия решений и улучшения производительности и отчетности». Уровни Реализации, Категории и Подкатегории – примеры метрик. Метрики дают информацию о состоянии безопасности организации путем сбора и корреляции показателей. Показатели – это «выражаемые количественно, поддающиеся наблюдению объективные данные, формирующие метрики». Показатели наиболее близко связаны с техническими средствами управления, такими как Информационные Ссылки.

Информация, извлеченная из метрик безопасности, показательна в разных аспектах состояния риска информационной безопасности организации. Поэтому отслеживание метрик безопасности и результатов бизнеса важно для понимания, как изменения в отдельных средствах управления безопасностью влияют на достижение целей бизнеса. Поскольку измерения важны, независимо от того, выполнены ли задачи бизнеса, обычно требуется оценивать вероятность достижения будущих целей путем опережающих измерений.

Способность организации определять причинно-следственные связи между информационной безопасностью и результатами бизнеса зависит от правильности и точности измерительных систем (например, составленных из ресурсов, выделенных в ID.AM-5). Таким образом измерительная система должна быть спроектирована, учитывая бизнес-требования и эксплуатационные расходы. Эксплуатационные расходы измерительной системы могут возрастать при увеличении точности измерений. Во избежание необоснованного завышения стоимости достаточно, чтобы точность и эксплуатационные расходы на систему соответствовали требуемой точности измерений для соответствующей бизнес-цели.

4.1 Корреляция с Результатами Бизнеса

Целью измерения информационной безопасности является корреляция информационной безопасности с бизнес целями (ID.BE-3), а также определение и количественная оценка причинно-следственных связей. К общим целям бизнеса относятся достижение результатов бизнеса/миссии, увеличение рентабельности и снижение риска для организации. Совокупность этих бизнес-целей может быть измерена в доходе на акцию и повышении цены/дохода на уровне топ-менеджмента организации: в виде выручки и чистой прибыли для высшего руководства; и в более частных показателях, таких как количество продуктов или часов, на более низких уровнях в организации.

Установить взаимосвязи между метриками информационной безопасности и бизнес-целями зачастую сложнее, чем простое измерить один результат по информационной безопасности. Существует большое количество и разнообразие факторов, влияющих на данную бизнес-цель. Например, банк,

занимающийся обслуживанием мелкой клиентуры, хочет увеличить количество клиентов, использующих он-лайн банкинг, и пытается сделать это, используя более строгую аутентификацию. Однако привлечение большего количества клиентов он-лайн банкинга также зависит от применения сообщений о доверенных он-лайн транзакциях, таргетирования на отдельные демографические группы клиентов, рекламирования этих он-лайн услуг в течение необходимого времени. Таким образом рост числа клиентов зависит от передачи сообщений, маркетинга, рекламы, информационной безопасности и других факторов.

Важным вопросом является относительная рентабельность мероприятий по информационной безопасности. Рентабельность означает достижение бизнес-цели с минимальными усилиями и расходами. Для определения рентабельности организация должна сначала иметь четкое представление о бизнес-целях, осознавать взаимосвязь между бизнес-целями и метриками информационной безопасности и взаимосвязь между бизнес-целями и факторами, не относящимися к информационной безопасности.

Влияние результатов по информационной безопасности на бизнес-цели зачастую неясно. Первичная роль информационной безопасности – сохранение ценности бизнеса путем защиты конфиденциальности, целостности и доступности информации, операций и процессов организации. Поэтому даже когда рентабельность или влияние результатов по информационной безопасности на бизнес-цели неясно, организация должна внимательно изменять свою программу по информационной безопасности. Зачастую результаты по информационной безопасности предотвращают неблагоприятные обстоятельства, такие как утечку данных.

Управление рисками организации – это анализ всех рисков при достижении данной бизнес цели. Обеспечение информационной безопасности является частью учета рисков организации при достижении ее бизнес-целей. Выделенные ниже Метрики Управления являются способом агрегации риска информационной безопасности, используя Ядро Концепции, обеспечивая учет информационной безопасности в управлении риском организации.

Способность организации определять причинно-следственные связи между результатами информационной безопасности и бизнес-целями также зависит от способности адекватно их разделять. Это одна из самых серьезных проблем, влияющих на измерение информационной безопасности. Особое внимание необходимо уделять определению, действительно ли данный результат информационной безопасности и бизнес-цель коррелируют. Обычно провести корреляцию показателей информационной безопасности высокоуровневым метрикам информационной безопасности легче, чем

установить корреляцию между метриками информационной безопасности и бизнес-целями.

4.2 Виды Измерений Информационной Безопасности

Метрики и показатели, относящиеся к Концепции сведены в Таблицу 1.

Таблица 1 – Виды измерений, предлагаемые в Концепции

Измерение	Что измеряется	Соответствующий Компонент Концепции	Вид измерений
Практики	Общий риск поведения руководства	Уровни Реализации	Метрика
Процесс	Специфические мероприятия по управлению рисками	Положения Концепции, включая семиэтапный Процесс (раздел 3.2) и использование ситуационно-обусловленного процесса (например, разделы 3.3 и 3.6)	Показатель
Руководство	Исполнение общих результатов по информационной безопасности	Ядро/Функции, Категории и Подкатегории Профиля	Метрика
Технический	Достижение отдельных результатов информационной безопасности	Информационные ссылки	Показатель

Уровни Реализации Концепции представляют собой качественную метрику всей деятельности по управлению риском информационной безопасности. Помимо качественной общей метрики 1–4 к метрикам деятельности также относятся индивидуальные характеристики Уровня Реализации в Процессе Управления Риском, Комплексная Программа Управления Риском, Внешнее Участие и Управление Рисками Цепи Поставок.

Положения, описанные в Уровнях Реализации, являются общими направлениями деятельности организации на высшем уровне, эти

мероприятия состоят из отдельных процессов, представляющих собой мероприятия по управлению рисками. Например, периодичность процесса обновления Профиля Концепции (этап 3) является показателем, отраженным в метрике Процесс Управления Риском. Аналогично показатель степени важности риска информационной безопасности (ID.GV-4) для процессов руководства и управления риском отражен в метрике Комплексная Программа Управления Риском. Наконец объем информации об угрозах и уязвимостях, полученный на совещаниях по обмену информацией и других источников, (ID.RA-2) отражен в метрике Внешнее Участие.

Результаты по информационной безопасности, содержащиеся в Ядре Концепции, составляют основу для полного набора метрик управления информационной безопасностью. Совокупность этих метрик соответствует снижению (или нет) риска информационной безопасности.

- Например, результат Функции Защиты – «разработка и реализация соответствующих мер безопасности для *обеспечения оказания услуг*…». Руководитель, ответственный за этот результат, может быть оценен по отстающей метрике доли периода работоспособности систем (т.е. обеспечения оказания услуг) с опережающей метрикой создания и доведения стратегии развития и реализации защиты данных.
- Соответственно, лицо, занимающееся Бизнес Процессом, может быть ответственно за Категорию Защиты Данных Функции Защиты (PR.DS) и ее Подкатегорий. Защита Данных означает, что «информация и записи (данные) управляются в соответствии со стратегией обработки рисков организации для защиты конфиденциальности, целостности и доступности информации». Лицо, занимающееся Бизнес Процессом, ответственное за Защиту Данных может оцениваться по опережающей метрике, отражающей издание политик и доведения их до персонала в соответствии как со стратегией рисков организации, так и целями обеспечения Конфиденциальности, Целостности и Доступности. Запаздывающие метрики для лица, занимающегося Бизнес Процессом, могут быть составлены из запаздывающих метрик, отражающих как Конфиденциальность, Целостность и Доступность управляются лицами, ответственными за Подкатегории Защиты Данных.
- Аналогично лицо, занимающееся Реализацией/Производственной деятельностью, ответственное за защиту хранимых данных (PR.DS-1), может быть оценено опережающей метрикой реализации защитных механизмов с запаздывающей метрикой, характеризующей, что защищенность данных доказывается отсутствием неавторизованной модификации, удаления или кражи данных организации. Это лицо, занимающееся Реализацией/Производственной деятельностью, может

удовлетворить цели PR.DS-1, используя Информационные ссылки и соответствующие показатели.

Каталоги средств управления, находящиеся в Информационных Ссылках, предлагают детальные технические показатели, объединенные в модули, образующие Концепцию. Например, организация, использующая средство управления безопасностью SP-28 из Специального Издания NIST Special Publication 800-53 для реализации Подкатегории PR.DS-1 могут нести ответственность за показатели проектирования, разработки/приобретения, реализации, управления, модернизации и списания следующего:

- Криптографические механизмы для разнообразных цифровых накопителей (внутренних жестких дисков, облачных жестких дисков, портативных накопителях, мобильных устройствах).
- Полное шифрование диска в отличие от отдельных структур данных (например, файлов, записей или полей).
- Сканирование файлообменников.
- Технологий с однократной записью и многократным считыванием.
- Защищенное автономное хранение вместо хранения он-лайн.

ПРИЛОЖЕНИЕ А. ФУНКЦИИ И СООТВЕТСТВУЮЩИЕ ИМ КАТЕГОРИИ ЯДРА КОНЦЕПЦИИ

Уникальный Идентификатор Функции	Функция	Уникальный Идентификатор Категории	Категория
		ID.AM	Управление Активами (Asset Management)
		ID.BE	Бизнес Среда (Business Environment)
		ID.GV	Руководство (Governance)
		ID.RA	Оценка Риска (Risk Assessment)
		ID.RM	Стратегия Управления Риском (Risk Management Strategy)
		ID.SC	Управление Риском Логистической Цепочки (Supply Chain Risk Management)
		PR.AC	Управление Доступом (Access Control)
		PR.AT	Повышение Осведомленности и Обучение (Awareness and Training)
		PR.DS	Защита Данных (Data Security)
		PR.IP	Процессы и Процедуры Защиты Информации (Information Protection Processes and Procedures)

Уникальный Идентификатор Функции	Функция	Уникальный Идентификатор Категории	Категория
		PR.MA	Техподдержка (Maintenance)
		PR.PT	Технология Защиты (Protective Technology)
		DE.AE	Аномалии и События (Anomalies and Events)
		DE.CM	Непрерывный Мониторинг Безопасности (Security Continuous Monitoring)
		DE.DP	Процессы Обнаружения (Detection Processes)
		RS.RP	Планирование Реагирования (Response Planning)
		RS.CO	Коммуникация (Communications)
		RS.AN	Анализ (Analysis)
		RS.MI	Подавление (Mitigation)
		RS.IM	Улучшение (Improvements)

Уникальный Идентификатор Функции	Функция	Уникальный Идентификатор Категории	Категория
RC	Восстановление (Recover)	RC.RP	Планирование Восстановления (Recovery Planning)
		RC.IM	Улучшение (Improvements)
		RC.CO	Коммуникации (Communications)

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
		ID.AM-1: Физическое оборудование и системы в организации инвентаризированы	– **CCS 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
		ID.AM-2: Программные платформы и приложения в организации инвентаризированы	– **CCS 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 – **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Коммуникации и потоки данных в организации отображены	– CCS CSC 1 – COBIT 5 DSS05.02 – ISA 62443-2-1:2009 4.2.3.4 – ISO/IEC 27001:2013 A.13.2.1 – NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Внешние информационные системы каталогизированы	– **COBIT 5** APO02.02 – **ISO/IEC 27001:2013** A.11.2.6 – **NIST SP 800-53 Rev. 4** AC-20, SA-9

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
		ID.AM-5: Ресурсы (например, оборудование, устройства, данные, время и программное обеспечение) приоритезированы на основе их классификации, критичности и ценности для бизнеса.	– **COBIT 5** APO03.03, APO03.04, 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
		ID.AM-6: Роли и сферы ответственности в области кибербезопасности для всех внутренних и внешних заинтересованных сторон (например, поставщиков, клиентов, партнеров) установлены	– **COBIT 5** APO01.02, 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
		ID.BE-1: Роль организации в цепочке поставок определена и сообщена	– **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 – **ISO/IEC 27001:2013** 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 критически важной инфраструктуре и ее отраслевом секторе определены и сообщены	– **COBIT 5** APO02.06, APO03.01 – **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Приоритеты для миссии, целей и деятельности организации установлены и сообщены	– **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

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
		ID.BE-4: Установлены зависимости и критические функции для предоставления критически важных услуг	– **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 состояний функционирования (например, при атаке, во время восстановления, во время нормального функционирования)	– **COBIT 5** 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-14
		ID.GV-1: Политика информационной безопасности организации установлена	– **COBIT 5** APO01.03, 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-е контроли всех семейств
		ID.GV-2: Роли и обязанности в области информационной безопасности скоординированы и согласованы с внутренними ролями и внешними партнерами	– **COBIT 5** APO13.02 – **ISA 62443-2-1:2009** 4.3.2.3.3 – **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 – **NIST SP 800-53 Rev. 4** PM-1, PS-7
		ID.GV-3: Правовые и нормативные требования в отношении кибербезопасности, в том числе	– **COBIT 5** MEA03.01, MEA03.04 – **ISA 62443-2-1:2009** 4.4.3.7

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
		обязательства в отношении конфиденциальности и гражданских свобод, поняты и управляются	– **ISO/IEC 27001:2013** A.18.1 – **NIST SP 800-53 Rev. 4** -1-е контроли всех семейств (за исключением PM-1)
		ID.GV-4: Процессы руководства и управления рисками направлены на устранение рисков кибербезопасности	– **COBIT 5** 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 – **NIST SP 800-53 Rev. 4** PM-9, PM-11
		ID.RA-1: Уязвимости активов идентифицированы и задокументированы	– **CCS CSC** 4 – **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 – **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 и информация об уязвимостях поступает с форумов и источников обмена информацией	– **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** PM-15, PM-16, SI-5
		ID.RA-3: Угрозы, как внутренние, так и внешние, идентифицированы и задокументированы	– **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

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
			– **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Потенциальные последствия для бизнеса и вероятности определены	– **COBIT 5** DSS04.02 – **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 – **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Угрозы, уязвимости, вероятности и воздействия используются для определения риска	– **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 расставлены по приоритетам	– **COBIT 5** APO12.05, APO13.02 – **NIST SP 800-53 Rev. 4** PM-4, PM-9
		ID.RM-1: Процессы управления рисками установлены, управляются и согласованы заинтересованными сторонами организации	– **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 – **ISA 62443-2-1:2009** 4.3.4.2 – **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Критерий принятия риска в организации определен и четко выражен	– **COBIT 5** APO12.06 – **ISA 62443-2-1:2009** 4.3.2.6.5 – **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: Определение толерантности к риску организации основывается на ее роли в	– **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
		критической инфраструктуре и анализе рисков для конкретных секторов	
		ID.SC-1: Процессы управления рисками в кибер-цепочке идентфицированы, устанавлены, оцениваются, управляются и согласовываются заинтересованными сторонами организации	– **CIS CSC**: 4.8 – **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 – **ISA 62443-3-3:2013**: – **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**: SA-9, SA-12, PM-9
		ID.SC-2: Идентифицировать, расставлять приоритеты и оценивать поставщиков и партнеров критически важных информационных систем, компонентов и услуг, используя процесс оценки рисков в кибер-цепочке поставок	– **CIS CSC**: – **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 – **ISA 62443-3-3**:2013: – **ISO/IEC 27001:2013**: A.15.2.1, A.15.2.2

Функция	Категория	Подкатегория	Взаимосвязь с другими требованиями
			– **NIST SP 800-53**: RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Поставщики и партнеры обязаны по контракту принять соответствующие меры, предназначенные для достижения целей программы информационной безопасности или плана управления рисками кибер-цепочки поставок	– **CIS CSC**: – **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 – **ISA 62443-3-3:2013**: – **ISO/IEC 27001:2013**: A.15.1.1, A.15.1.2, A.15.1.3 – **NIST SP 800-53**: SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Поставщики и партнеры контролируются, чтобы подтвердить, что они выполнили свои обязательства в соответствии с требованиями. Проводятся обзоры аудитов, сводки результатов тестов или другие эквивалентные оценки поставщиков	– **CIS CSC**: – **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**: 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 критичными поставщиками	– **CIS CSC**: 19.7, 20.3 – **COBIT 5**: DSS04.04 – **ISA 62443-2-1:2009**: 4.3.2.5.7, 4.3.4.5.11

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
			– **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**: CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
		PR.AC-1: Идентификационные и учетные данные выдаются, управляются, верифицируются, аннулируются и проверяются для авторизованных устройств, пользователей и процессов	– **CCS CSC** 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.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 – **NIST SP 800-53 Rev. 4** AC-2, IA Family
		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.11.1.4, A.11.1.6, A.11.2.3 – **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE- 5, PE-6, PE-9
		PR.AC-3: Удаленный доступ управляется	– **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

Функция	Категория	Подкатегория	Взаимосвязь с другими требованиями
			– **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 – NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
		PR.AC-4: Разрешения на доступ и авторизация управляются, с использованием принципов наименьших привилегий и разделения обязанностей	– **CCS CSC** 12, 15 – **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 – **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Целостность сети защищена, включая сегрегацию сети, где это необходимо	– **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 – **NIST SP 800-53 Rev. 4** AC-4, SC-7
		PR.AC-6: Идентификационные данные проверяются и привязываются к учетным данным, а при необходимости утверждаются во взаимодействиях	– **CIS CSC**: CSC 5, 12, 14, 16 – **COBIT 5**: DSS05.04, DSS05.05, DSS05.07, DSS06.03, BAI08.03 – **ISA 62443-2-1:2009**: 4.3.2.4.2, 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.4 – **ISA 62443-3-3:2013**: SR 1.4, SR 1.5, SR 2.1, SR 2.2, SR 2.3 – **ISO/IEC 27001:2013**: A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
			– **NIST SP 800-53**: AC-2, AC-3, AC-5, AC-6, AC-16, AC-19, AC-24, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AT-1: Все пользователи проинформированы и обучены	– **CCS CSC** 9 – **COBIT 5** APO07.03, BAI05.07 – **ISA 62443-2-1:2009** 4.3.2.4.2 – **ISO/IEC 27001:2013** A.7.2.2 – **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Привилегированные пользователи понимают роли и ответственность	– **CCS CSC** 9 – **COBIT 5** APO07.02, 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: Внешние заинтересованные стороны (например, поставщики, клиенты, партнеры) понимают роли и ответственность	– **CCS CSC** 9 – **COBIT 5** APO07.03, APO10.04, APO10.05 – **ISA 62443-2-1:2009** 4.3.2.4.2 – **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 – **NIST SP 800-53 Rev. 4** PS-7, SA-9
		PR.AT-4: Высшее руководство понимает роли и ответственность	– **CCS CSC** 9 – **COBIT 5** APO07.03 – **ISA 62443-2-1:2009** 4.3.2.4.2

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
			– **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: Сотрудники физической и информационной безопасности понимают роли и ответственность	– **CCS CSC** 9 – **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, PM-13
		PR.DS-1: Данные в состоянии покоя защищены	– **CCS CSC** 17 – **COBIT 5** APO01.06, BAI02.01, BAI06.01, 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** SC-28
		PR.DS-2: Данные при передаче защищены	– **CCS CSC** 17 – **COBIT 5** APO01.06, 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
		PR.DS-3: Активы формально управляются при удалении, передаче и утилизации.	– **COBIT 5** BAI09.03 – **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
			– **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.11.2.7 – **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Поддерживаются адекватные возможности для обеспечения доступности	– **COBIT 5** APO13.01 – **ISA 62443-3-3:2013** SR 7.1, SR 7.2 – **ISO/IEC 27001:2013** A.12.3.1 – **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Защита от утечки данных реализована	– **CCS CSC** 17 – **COBIT 5** APO01.06 – **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.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 программного обеспечения, встроенного	– **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 – **NIST SP 800-53 Rev. 4** SI-7

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
		программного обеспечения и целостности информации.	
		PR.DS-7: Среда (ы) разработки и тестирования отделены от производственной среды	– **COBIT 5** 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	– **CIS CSC**: CSC 3.3 – **COBIT 5**: BAI03.05.4 – **ISA 62443-2-1:2009**: 4.3.4.4.4 – **ISA 62443-3-3:2013**: – **ISO/IEC 27001:2013**: A.11.2.4 – **NIST SP 800-53**: SA-10, SI-7
		PR.IP-1: Базовая конфигурация информационных технологий / промышленных систем управления создается и поддерживается с учетом соответствующих принципов безопасности (например, концепция минимальной функциональности)	– **CCS CSC** 3, 10 – **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

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
	организационными подразделениями), процессы и процедуры поддерживаются и используются для управления защитой информационных систем и активов.	**PR.IP-2**: Реализован жизненный цикл разработки систем (SDLC) для управления системами	– **COBIT 5** APO13.01 – **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** SA-3, SA-4, SA-8, SA- 10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Процессы контроля изменений конфигурации реализованы	– **COBIT 5** BAI06.01, BAI01.06 – **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: Резервные копии данных создаются, поддерживаются и периодически проверяются	– **COBIT 5** APO13.01 – **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.17.1.2A.17.1.3, A.18.1.3 – **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Политика и положения относительно физической безопасности для	– **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

Функция	Категория	Подкатегория	Взаимосвязь с другими требованиями
		организационных активов соблюдаются	– **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 – **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: Процессы защиты постоянно улучшаются	– **COBIT 5** APO11.06, 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 – **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR- 8, PL-2, PM-6
		PR.IP-8: Эффективность технологий защиты доводится до соответствующих сторон	– **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	– **COBIT 5** 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 – **NIST SP 800-53 Rev. 4** CP-2, IR-8

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
		восстановление) созданы и управляются	
		PR.IP-10: Планы реагирования и восстановления проверены	– **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 работы с персоналом (например, ограничение доступа, проверка персонала)	– **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.7.3.1, A.8.1.4 – **NIST SP 800-53 Rev. 4** PS Family
		PR.IP-12: План управления уязвимостями разработан и внедрен	– **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 – **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
		PR.MA-1: Техническое обслуживание и ремонт организационных активов выполняются и регистрируются своевременно с использованием утвержденных и контролируемых инструментов	– **COBIT 5** BAI09.03 – **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 – **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
	соответствии с политиками и процедурами.	**PR.MA-2**: Удаленное обслуживание организационных активов одобрено, зарегистрировано и выполняется способом, который предотвращает несанкционированный доступ	– **COBIT 5** DSS05.04 – **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 – **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 – **NIST SP 800-53 Rev. 4** MA-4
		PR.PT-1: Записи аудита / журналов событий определяются, документируются, внедряются и проверяются в соответствии с политикой	– **CCS CSC** 14 – **COBIT 5** APO11.04 – **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: Съемные носители информации защищены, и их использование ограничено в соответствии с политикой	– **COBIT 5** DSS05.02, APO13.01 – **ISA 62443-3-3:2013** SR 2.3 – **ISO/IEC 27001:2013** 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-4, MP-5, MP-7
		PR.PT-3: Принцип наименьшей функциональности заложен в настройке систем для обеспечения	– **COBIT 5** DSS05.02 – **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2,

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
		только необходимых возможностей	4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 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	– **CCS CSC** 7 – **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 – **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
		PR.PT-5: Системы работают в заранее определенных функциональных состояниях для достижения доступности (например, под нагрузкой, под атакой, во время восстановления, в нормальных условиях).	– **CIS CSC**: – **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**: CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
Обнаружение (DE)	**Аномалии и События (DE.AE)**: Аномальная активность обнаруживается своевременно, а потенциальное влияние событий понимается	**DE.AE-1**: Устанавливается и управляется базовый уровень сетевых операций и ожидаемых потоков данных для пользователей и систем	– **COBIT 5** DSS03.01 – **ISA 62443-2-1:2009** 4.4.3.3 – **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	– **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.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 агрегируются и коррелируются из нескольких источников и сенсоров	– **ISA 62443-3-3:2013** SR 6.1 – **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR- 5, IR-8, SI-4
		DE.AE-4: Влияние событий определяется	– **COBIT 5** APO12.06 – **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI - 4
		DE.AE-5: Установлены пороги оповещения об инциденте	– **COBIT 5** APO12.06 – **ISA 62443-2-1:2009** 4.2.3.10 – **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
		DE.CM-1: Сеть контролируется для обнаружения потенциальных событий кибербезопасности	– **CCS CSC** 14, 16 – **COBIT 5** DSS05.07 – **ISA 62443-3-3:2013** SR 6.2

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
	Информационная система и активы контролируются с через определенные промежутки времени для выявления событий кибербезопасности и проверки эффективности защитных мер.		– **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 контролируется для обнаружения потенциальных событий кибербезопасности	– **ISA 62443-2-1:2009** 4.3.3.3.8 – **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE- 20
		DE.CM-3: Деятельность персонала отслеживается для выявления потенциальных событий кибербезопасности	– **ISA 62443-3-3:2013** SR 6.2 – **ISO/IEC 27001:2013** A.12.4.1 – **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Вредоносный код обнаруживается	– **CCS CSC** 5 – **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
		DE.CM-5: Неавторизованный мобильный код обнаруживается	– **ISA 62443-3-3:2013** SR 2.4 – **ISO/IEC 27001:2013** A.12.5.1 – **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
		DE.CM-6: Активность внешних поставщиков услуг контролируется	– **COBIT 5** APO07.06 – **ISO/IEC 27001:2013** A.14.2.7, A. 15.2.1

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
		для обнаружения потенциальных событий кибербезопасности	– **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA- 9, SI-4
		DE.CM-7: Выполняется мониторинг неавторизованных персонала, подключений, устройств и программного обеспечения	– **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: Сканирование уязвимостей выполняется	– **COBIT 5** BAI03.10 – **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
		DE.DP-1: Роли и обязанности по выявлению четко определены для обеспечения подотчетности	– **CCS CSC** 5 – **COBIT 5** DSS05.01 – **ISA 62443-2-1:2009** 4.4.3.1 – **ISO/IEC 27001:2013** A.6.1.1 – **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Деятельность по обнаружению соответствует всем применимым требованиям	– **ISA 62443-2-1:2009** 4.4.3.2 – **ISO/IEC 27001:2013** A.18.1.4 – **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Процессы обнаружения тестируются	– **COBIT 5** APO13.02 – **ISA 62443-2-1:2009** 4.4.3.2

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
			– **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, PM-14, SI-3, SI-4
		DE.DP-4: Информация об обнаружении событий передается соответствующим сторонам	– **COBIT 5** APO12.06 – **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 – **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Процессы обнаружения постоянно совершенствуются	– **COBIT 5** APO11.06, 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
	Планирование Реагирования (RS.RP): Процессы и процедуры реагирования выполняются и поддерживаются для обеспечения своевременного реагирования на	**RS.RP-1**: План реагирования выполняется во время или после события	– **COBIT 5** BAI01.10 – **CCS CSC** 18 – **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

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
	обнаруженные события кибербезопасности		
		RS.CO-1: Персонал знает свои роли и порядок действий, при выполнении мероприятий по реагированию	– **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.16.1.1 – **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-81
		RS.CO-2: События сообщаются в соответствии с установленными критериями	– **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 передается в соответствии с планами реагирования	– **ISA 62443-2-1:2009** 4.3.4.5.2 – **ISO/IEC 27001:2013** A.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	– **ISA 62443-2-1:2009** 4.3.4.5.5 – **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	– **NIST SP 800-53 Rev. 4** PM-15, SI-5

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
		широкой осведомленности о кибербезопасности	
		RS.AN-1: Уведомления от систем обнаружения исследуются	– **COBIT 5** 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: Влияние инцидента понимается	– **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.16.1.6 – **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Испоользуются криминалистические техники	– **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	– **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.MI-1: Инциденты локализируются	– **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.16.1.5

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
	расширения ущерба от события, снижения его последствий и устранения инцидента.		– **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Смягчаются последствия от инцидента	– **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 смягчаются или документируются как принятые риски	– **ISO/IEC 27001:2013** A.12.6.1 – **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
		RS.IM-1: Планы реагирования включают 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 – **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Стратегии реагирования обновляются	– **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Планирование Восстановления (RC.RP): Процессы и процедуры восстановления выполняются и поддерживаются для обеспечения своевременного восстановления систем или	**RC.RP-1**: План восстановления выполняется во время или после события	– **CCS CSC** 8 – **COBIT 5** DSS02.05, DSS03.04 – **ISO/IEC 27001:2013** A.16.1.5 – **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8

Функция	Категория	Подкатегирия	Взаимосвязь с другими требованиями
	активов, затронутых событиями кибербезопасности		
		RC.IM-1: Планы восстановления включают извлеченные уроки	– **COBIT 5** BAI05.07 – **ISA 62443-2-1:2009** 4.4.3.4 – **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Стратегии восстановления обновляются	– **COBIT 5** BAI07.08 – **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.CO-1: Связи с общественностью управляются	– **COBIT 5** EDM03.02
		RC.CO-2: Репутация после события восстанавливается	– **COBIT 5** MEA03.02
		RC.CO-3: Действия по восстановлению передаются внутренним заинтересованным сторонам, а также высшему руководству и компанде управления	– **NIST SP 800-53 Rev. 4** CP-2, IR-4

Информация, касающаяся информационных ссылок, описанных в представленной выше таблице, может быть найдена в следующих местах:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org
- ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800-53r4.