МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**



**МОСКОВСКИЙ**

**ПОЛИТЕХ**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Информационная безопасность»

Проектная деятельность

Тема: “Оценка зрелости по фреймворку **O-ISM3 2017**”

Выполнил: Студент 2 курса гр. 191-331

Травкин Александр

Научный руководитель:

Агеева Елена Александровна

2020 г. Москва

**Оглавление**

**Часть 1**3

Вступление3

Модель O-ISM33

Уровни управления безопасностью4

Уровни зрелости и метрики4

Вывод6

**Часть 27**

Описание процесса7

Общие процессы7

Стратегические процессы13

Тактические процессы17

Операционные процессы24

**Часть 1**

**Вступление**

Постановка задачи по внедрению и продвижению любого процесса управления в организации должна соответствовать уровню организационного и технологического развития, и в частности, процессов обеспечения безопасности. Требования к реализации мероприятий по информационной безопасности должны формулироваться с учетом **уровня зрелости** этих процессов в конкретной организации.  То есть, не стоит пытаться требовать внедрить мощную современную технологию, если уровень организации не соответствует уровню технологии. Этот вывод относится и к использованию нового оборудования. Практически всегда современные технические средства требуют чрезвычайно высокого уровня обслуживания. Если персонал не обладает необходимыми для корректной работы навыками, то приобретение данного оборудования окажется бессмысленным: оно либо потеряет свои параметры, либо просто будет испорчено.

Для определения стадии организационного и технологического развития организации и ее процессов существует понятие «**модель зрелости**». Модель зрелости используется как инструмент измерения состояния процесса на основе набора **метрик** (их мы рассмотрим дальше), которые представляют собой определенные характеристики. Оценка этих метрик по оговоренной шкале позволяет понять состояние процессов организации, которая и будет характеризовать уровень зрелости. После получения оценки зрелости можно выработать необходимые мероприятия для повышения зрелости процессов и организации в целом.

**Модель O-ISM3**

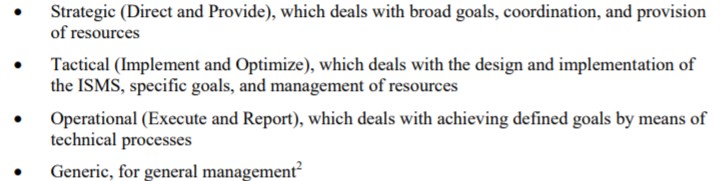
Модель  «**Open Information Security Management Maturity Model (O-ISM3)**», разработана независимым консорциумом The Open Group ([www.opengroup.org](http://www.opengroup.org/)).

Модель О-ISM3 оценивает зрелость функционирования существующих процессов системы управления информационной безопасности (СУИБ) организации. Модель разрабатывалась как методика, которая поможет менеджерам информационной безопасности оценить свою собственную рабочую среду и запланировать процессы управления безопасностью

Модель O-ISM3 требует, чтобы процессы СУИБ были задокументированы, измерялись и управлялись. O-ISM3 так же требует, чтобы были зафиксированы бизнес-цели организации, и на их основе определены цели и задачи безопасности. Отличительной особенностью модели O-ISM3 является то, что она основана на оценке зрелости каждого из применяемых в СУИБ контролей (мер безопасности). Т.е. чтобы управлять контролем (согласно процессному подходу) необходимо оценивать уровень его зрелости.

**Уровни управления безопасностью**

O-ISM3 определяет **четыре** уровня управления безопасностью на основе того, что каждый уровень процесса отчитывается перед вышестоящим, поэтому только стратегический уровень отчитывается перед ИТ-директором. Если ИТ-директор принимает ответственность тактического уровня, это происходит плавно. На картинке ниже перечислены эти уровни:



**Уровни зрелости и метрики**

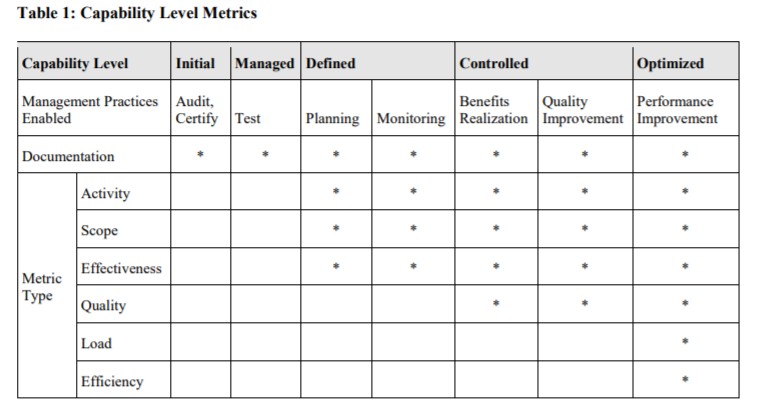
В модели O-ISM3 процессы системы управления классифицируются по **пяти** уровням зрелости:

* Уровень зрелости 1 – Начальный (**Initial**);
* Уровень зрелости 2 – Управляемый (**Managed**);
* Уровень зрелости 3 – Описанный (**Defined**);
* Уровень зрелости 4 – Контролируемый (**Controlled**);
* Уровень зрелости 5 – Оптимизированный (**Optimized**).

Метрики подразделяются на **шесть** возможных типов (**Activity, Scope**, **Effectiveness**, **Load**, **Quality**, **Efficiency**) и описывают эффективность выбранного метода управления. С точки зрения аудитора уровень, достигнутый процессом, зависит от документации, и метрики использованной для управления им.

Таблица 1 определяет, какие метрики необходимы для того, чтобы процесс достиг каждого уровня возможностей, и его соответствующее сопоставление с методами управления.

Метрики позволяют переходить из базового состояния в оптимизированное состояние. Наличие документации - необходимое условие для достижения любого уровня возможностей.



**Вывод**

Модель O-ISM3 разработана для любых типов организаций, коммерческих фирм, неправительственных организаций, производственных предприятий:

* Применима к любой организации независимо от размера, контекста и ресурсов;
* Требует высокой квалификации менеджеров по безопасности и высокой детализации процессов безопасности;
* Позволяет организациям расположить по приоритетам и оптимизировать свои инвестиции в безопасность;
* Позволяет непрерывно улучшать СУИБ на основе использования метрик.

**Часть 2**

**Описание процесса**

В контексте O-ISM3 безопасность - это результат процесса. Чем лучше процесс обеспечения безопасности, тем лучше достигается защита от имеющихся ресурсов.

**Общие процессы**

Общие процессы обеспечивают необходимую инфраструктуру для внедрения, оценки и совершенствования процессов ISM (Information Security Management). Они включают в себя:

•Управление знаниями для сбора и обмена информацией по управлению безопасностью в рамках СУИБ;

•СУИБ и бизнес аудит для проверки соответствия внутренней политике и нормативным требованиям;

•Разработка/эволюция СУИБ для оценки того, достигают ли текущие процессы поставленных целей управления безопасностью.

**GP-1: Knowledge Management**

|  |  |
| --- | --- |
|  | **GP-1: Knowledge Management** |
| **Описание** | Этот процесс собирает, анализирует, хранит, передает и делится знаниями внутри организации. Он поддерживает СУИБ, определяя стандарты качества документов, организацию и распределение документов и записей, связанных с конкретными процессами, и помогает поддерживать их в актуальном состоянии, требуя истечения срока действия документов и их пересмотра. В то время как знания могут храниться с помощью экспертных систем, Вики-сайтов и платформ совместной работы, документы считаются наиболее широко используемым хранилищем знаний. |
| **Ценность/значение** | Процессы обеспечения безопасности реализуются надежным и воспроизводимым способом, когда соответствующие документы являются атрибутивными, актуальными, извлекаемыми и подлежащими процессу проверки, поскольку документы являются ключевыми для хранения и передачи знаний. Этот процесс повышает эффективность, уменьшая необходимость повторного приобретения знаний. |
| **Входные данные** | Экспертное знание, описание процесса, обязанности и сфера применения. |
| **Выходные данные** | Перечень рецензируемых документов, перечень утвержденных новых и обновленных документов, список распространяемых и вышедших из эксплуатации версий документов.   * Отчеты: документы, отражающие резюме и интерпретацию результатов процесса. * Шаблоны и формы: общий макет и формат вида документа. * Планы: документы, определяющие объем процесса, ресурсы, необходимые для его создания и выполнения, а также способы его настройки. * Контрольные списки: документы, обеспечивающие последовательное выполнение сложной задачи. |
| **Метрические описания** | N/A |

**GP-2: ISMS and Business Audit**

|  |  |
| --- | --- |
|  | **GP-2: ISMS and Business Audit** |
| **Описание** | Этот процесс проверяет, является ли:   * Технологическая документация, входные данные, выходные данные и мероприятия соответствуют стандартам, законам, нормативным актам и внутренней политике; * Существующая схема делегирования полномочий соответствует правилам TPSRSR; * Входные данные процессов, действия и результаты соответствуют их документации.   Он может быть применен для проверки соответствия и возможностей всех процессов или репрезентативной выборки. Аудитор должен планировать, документировать и проводить аудит, чтобы свести к минимуму вероятность получения неверного заключения, следуя соответствующим профессиональным рекомендациям. |
| **Ценность/значение** | Инциденты, возникающие из-за неисправностей в СУИБ, можно предотвратить, проверив систему и приняв меры для решения проблем, связанных с улучшением, например:   * Соответствие бизнес-процессов действующим нормативным актам; * Схема делегирования полномочий по правилам TPSRSR (transparency, partitioning, supervision, rotation and separation of responsibilities - прозрачность, разделение, надзор, ротация и разделение обязанностей); * Реализация ISMS в соответствии с определением. |
| **Входные данные** | * GP-024: политика ИБ; * SSP-041: политика TPSRSR; * ISM документация процесса, прошедшего аудит; * Результаты каждого проверяемого процесса; * Результаты предыдущих аудитов. |
| **Выходные данные** | * Отчет Об Аудите Процесса; * Отчет об аудите ISM; * Отчет о сертификации ISM; * ISM Certification Assessment TPSRSR Rules Report; * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**GP-3: ISM Design and Evolution** и **GP-1: Knowledge Management**-это основные процессы, необходимые для “загрузки” информационной системы управления O-ISM3.

**GP-3: ISM Design and Evolution**

|  |  |
| --- | --- |
|  | **GP-3: ISM Design and Evolution** |
| **Описание** | Этот процесс проверяет, соответствует ли существующий операционный процесс потребностям организации и целям соответствия, выраженным в виде бизнес -целей, или нет. Он также проверяет, работает ли процесс лучше и эффективнее, чем это было раньше. Область применения включает в себя следующие области:   * Организационная миссия и окружающая среда; * Соответствие законодательным/нормативным требованиям; * Защита конфиденциальности, как сотрудников, так и клиентов; * Защита интеллектуальной собственности.   Этот процесс выбирает наиболее подходящие операционные процессы для достижения целей безопасности. |
| **Ценность/значение** | Разработка конкретных бизнес-целей требует стратегического понимания окружающей среды и бизнес-целей организации. Бизнес-цели обеспечивают основу для политики и целей ИБ. Каждая организация имеет разные цели безопасности, действует в разных управляемых ею доменах и имеет разные ресурсы. Правильный выбор процессов даст хорошую отдачу от инвестиций в безопасность. Эффективность процессов и их результативность могут со временем снижаться, если в организации не предпринимаются постоянные усилия по достижению более высоких уровней потенциала. |
| **Входные данные** | ***Организационные цели и стратегия***   * GP-017: политика управления жизненным циклом; * GP-024: политика ИБ; * Цели информационной безопасности (TSP-3); * Выделение ресурсов для обеспечения информационной безопасности (SSP-6); * Инвентаризация основных средств (OSP-3); * Отчеты об инцидентах (OSP-24); * Отчеты о вторжениях (OSP-24); * Судебно-медицинские заключения (OSP-25); * Резервный протокол испытаний (OSP-10); * Отчет об испытаниях повышенной надежности и доступности (OSP-26); * Отчет по испытанию непрерывности деятельности (OSP-15); * Отчет о возможностях потенциальных злоумышленников (TSP-14); * Потенциальные злоумышленники доклад о Контршпионаже (TSP-14); |
| **Выходные данные** | * Внутренние и внешние угрозы и уязвимости для целей бизнеса и безопасности в каждом управляемом ИТ домене; * Приемлемые внутренние и внешние угрозы и уязвимости для целей бизнеса и безопасности в каждом управляемом ИТ домене; * Отчет об угрозах страхования (TSP-13); * Рекомендуемые инвестиции в существующие и новые процессы ISM для каждого управляемого домена IT (SSP-6); * Определение процессов управления информационной безопасностью (включая приоритеты и необходимые инвестиции); * Отчет об оценке целей; * Отчет о стратегии; * Реализация преимуществ; |
| **Метрические описания** | N/A |

**Стратегические процессы**

Стратегическое управление несет ответственность за выбор и проектирование услуг, обеспечивающих ценность в рамках параметров затрат и рисков организации. Стратегическое управление подотчетно заинтересованным сторонам за использование ресурсов в рамках механизмов управления. Таким образом, заказчиками стратегического управления являются внешние и, возможно, внутренние заинтересованные стороны.

Стратегическое управление выполняет следующие конкретные цели и обязанности в отношении безопасности:

* Обеспечивает руководство и координацию деятельности:
* Информационной безопасностью
* Безопасностью рабочего места
* Физической безопасностью
* Взаимодействием с организационными подразделениями
* Рассматривает и совершенствует ISM, включая назначение руководителей и внутренних и внешних аудиторов;
* Определяет отношения с другими организациями, такими как партнеры, поставщики и подрядчики;
* Выделяет ресурсы для обеспечения информационной безопасности;
* Определяет цели обеспечения безопасности в соответствии с бизнес целями, защищая интересы заинтересованных сторон;
* Определяет организационную схему делегирования полномочий.

**SSP-1: Report to Stakeholders**

|  |  |
| --- | --- |
|  | **SSP-1: Report to Stakeholders** |
| **Описание** | Ежегодный или ежеквартальный отчет перед заинтересованными сторонами о соблюдении применимых нормативных актов, а также об исполнении бюджетных ассигнований и целевых показателей безопасности. |
| **Ценность/значение** | Для принятия решений о будущих инвестициях и деятельности организации заинтересованным сторонам требуется информация о результатах деятельности, включая значительные достижения в области ИБ. |
| **Входные данные** | * Отчет о безопасности оперативной информации (OSP-1); * Тактический Отчет по информационной безопасности (TSP-1); * Отчеты по метрикам (из остальных стратегических процессов). |
| **Выходные данные** | * Отчет о стратегической информационной безопасности (для заинтересованных сторон); * Отчет по метрикам (для заинтересованных сторон). |
| **Метрические описания** | N/A |

**SSP-2: Coordination**

|  |  |
| --- | --- |
|  | **SSP-2: Coordination** |
| **Описание** | Координация между руководством организации и руководством функции обеспечения безопасности. |
| **Ценность/значение** | Координация между персоналом, ответственным за безопасность (информационную, физическую, личную) и организационными руководителями необходима для обеспечения поддержки всей организации и оказания помощи организации в достижении ее целей и оптимизации ресурсов. |
| **Входные данные** | * Информационная безопасность и другие цели обеспечения безопасности. |
| **Выходные данные** | * Протокол заседания; * Отчет по метрикам (SSP-1); * Процессы ИБ, поддерживающие организацию. |
| **Метрические описания** | N/A |

**SSP-4: Define Division of Duties Rules (определение правил разделения обязанностей)**

|  |  |
| --- | --- |
|  | **SSP-4: Define Division of Duties Rules** |
| **Описание** | В этом процессе определяются правила распределения и управления обязанностями по обеспечению безопасности в рамках всей организации. |
| **Ценность/значение** | Четкие правила распределения обязанностей могут улучшить использование ресурсов и снизить риск инцидентов безопасности, помогая защитить организацию от внутренних угроз. |
| **Входные данные** | * Организационные цели и стратегия. |
| **Выходные данные** | * SSP-041: политика TPSRSR * Отчет по метрикам (SSP-1) |
| **Метрические описания** | N/A |

**SSP-6: Allocate Resources for Information Security (распределение ресурсов для обеспечения информационной безопасности)**

|  |  |
| --- | --- |
|  | **SSP-6: Allocate Resources for Information Security** |
| **Описание** | Этот процесс выделяет ресурсы для людей, бюджета и объектов для тактического и оперативного управления. |
| **Ценность/значение** | Внедрение ISM требует инвестиций в процессы тактического и оперативного управления. |
| **Входные данные** | * Рекомендуемые инвестиции в существующие и новые процессы ISM для каждого управляемого домена IT (GP-3); * Отчет об оценке инцидента (TSP-4). |
| **Выходные данные** | * Ресурсы, выделяемые на управление информационной безопасностью; * Бюджет информационной безопасности (TCP-2, GP-3, OSP-2); * Отчет по метрикам (SSP-1). |
| **Метрические описания** | N/A |

**Тактические процессы**

Стратегический менеджмент является заказчиком тактического менеджмента в отношении процессов ISM. Тактический менеджмент подотчетен стратегическому менеджменту за выполнение ISM и за использование ресурсов.

Тактическое управление имеет следующие конкретные цели и обязанности:

* Обеспечение обратной связи со стратегическим менеджментом;
* Управление бюджетом, персоналом и другими ресурсами, выделяемыми на обеспечение информационной безопасности;
* Определение среды для оперативного управления:
* Цели безопасности и классификация активов;
* Архитектура безопасности и управление жизненным циклом;
* Управление уровнем обслуживания (определение систем измерений и метрик);
* Управление страхованием;
* Кадровая безопасность;
* Информационная операция.

**TSP-1: Report to Strategic Management**

|  |  |
| --- | --- |
|  | **TSP-1: Report to Strategic Management** |
| **Описание** | Регулярный отчет о результатах обеспечения безопасности и использовании выделенных ресурсов. |
| **Ценность/значение** | Для демонстрации эффективности, действенности и результативности ISM требуется отчет перед стратегическим руководством. |
| **Входные данные** | * Отчет о безопасности оперативной информации (ОSP-1); * Отчеты по метрикам (из всех тактических процессов); * ISM Performance and Return on Investment Report (TSP-4). |
| **Выходные данные** | * Отчет о тактической информационной безопасности (SSP-1). |
| **Метрические описания** | N/A |

**TSP-2: Manage Allocated Resources (Управление выделенными ресурсами)**

|  |  |
| --- | --- |
|  | **TSP-2: Manage Allocated Resources** |
| **Описание** | Тактическое управление распределяет ресурсы между всеми процессами тактического и оперативного управления. |
| **Ценность/значение** | Планирование и контроль при распределении ресурсов необходимы для обеспечения того, чтобы ISM был сконфигурирован для достижения целей безопасности. |
| **Входные данные** | * Бюджет информационной безопасности (SSP-6); * Запрос ресурсов информационной безопасности (из тактических и оперативных процессов). |
| **Выходные данные** | * Назначение ресурсов информационной безопасности (тактическим и оперативным процессам); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**TSP-3: Define Security Targets and Security Objectives**

|  |  |
| --- | --- |
|  | **TSP-3: Define Security Targets and Security Objectives** |
| **Описание** | Этот процесс определяет цели безопасности для конкретных бизнес-целей, цели безопасности для связанного управляемого ИТ-домена и соответствующие политики/стандарты. Учитываются бизнес, персонал, контроль доступа, приоритет, долговечность, качество информации и технические требования. |
| **Ценность/значение** | Определение целей безопасности и задач безопасности для каждого управляемого домена ИТ обеспечивает основу для построения процессов ISM. |
| **Входные данные** | * Политика информационной безопасности (GP-24, GP-3). |
| **Выходные данные** | * Цели информационной безопасности (TSP-4, GP-3, OSP-2, OSP-8, OSP-9, OSP-20); * Требования к информации и классификация (документация); * Политика приемлемого использования (TSP-10, TSP-11); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**TSP-4: Service Level Management (управление уровнем обслуживания)**

|  |  |
| --- | --- |
|  | **TSP-4: Service Level Management** |
| **Описание** | Определяет метрики процессов для других процессов в ISM. Проверяет пороговые значения для каждой метрики процесса. Контролирует метрические измерения и запрашивает действия по наблюдению за аномальными метрическими измерениями. Передает входные данные для целей тестирования другим процессам и запрашивает действия, если они не дают ожидаемых результатов. Предлагает исправления и улучшения процессов. Предполагает улучшение использования ресурсов процессов. Оценивает стоимость инцидентов. |
| **Ценность/значение** | Информация, полученная из метрик, обеспечивает объективный способ оценки ISM и ее составляющих процессов. |
| **Входные данные** | * Цели информационной безопасности (TSP-3); * Журналы физического присутствия (OSP-14); * Журналы условий окружающей среды (ОСП-14); * Отчет об осведомленности о безопасности (TSP-4); * Журнал отклоненных и предоставленных запросов доступа (OSP-12); * Отчет о попытках несанкционированного доступа (OSP-11); * Отчет об уровне развертывания и обновления защиты от вредоносных программ (OSP-17); * Отчет о правилах фильтрации (TSP-4); * Отчет о вторжении (OSP-24); * Судебно-медицинское заключение (ОSP-25); * Отчеты по метрикам (из всех операционных процессов). |
| **Выходные данные** | * Устранение ошибок и неисправностей в технологических процессах; * Определение метрик процессов (для каждого операционного процесса); * Отчет об оценке инцидентов (SSP-6); * ISM Performance and Return on Investment Report (TSP-1, SSP-6); * Отчет по метрикам (TSP-1). |
| **Метрические описания** | N/A |

**TSP-6: Security Architecture**

|  |  |
| --- | --- |
|  | **TSP-6: Security Architecture** |
| **Описание** | Этот процесс управляет:   * Архитектурой ИТ-безопасности организации, использующей шаблоны безопасности для обеспечения универсальных, масштабируемых решений, которые позволяют создавать и развивать новые информационные системы, обслуживающие потребности организации; * Важными логическими управляемыми ИТ-доменами и их жизненными циклами; в каждой среде может существовать отдельный экземпляр некоторых операционных процессов. |
| **Ценность/значение** | Идентификация и определение различных управляемых ИТ-областей и систем, сгруппированных в них, необходимы для обеспечения реализации соответствующих процессов управления окружающей средой и жизненным циклом. Внедрение моделей безопасности снижает затраты и риски, а также повышает гибкость при внедрении информационных систем. |
| **Входные данные** | * GP-017: политика управления жизненным циклом (документация); * Работа с управляемыми доменами в организации; * Состояния и события, отмечающие переход состояний в каждом управляемом ИТ-домене. |
| **Выходные данные** | * Определение управляемых доменов и жизненных циклов (документация); * Документ Соответствия Архитектуры Безопасности; * Системы / приложения, свободные от единичных точек отказа; * Системы / приложения, максимальное количество одновременных сеансов которых ограничено; * Системы/приложения, учетные данные которых для первого входа в систему не предсказуемы; * Системы/приложения с настроенными задержками между последовательными отказами в входе в систему; * Системы/приложения, срок действия сеансов которых истек; * Сбой систем/приложений с ограниченным последовательным входом в систему; * Системы / приложения, качество учетных данных которых контролируется паролем; * Системы/приложения, требующие изменения учетных данных пароля при первом входе в систему; * Изменения состояния, подлежащие контролю изменений; * Процентная доля информационных систем, охваченных этим процессом; * Информационные системы, подверженные очистке при изменении состояния; * Информационные системы, подверженные упрочнению при изменении состояния; * Разрабатываемые информационные системы тестируются на соответствие требованиям; * Обученный персонал службы безопасности; * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**TSP-13: Insurance Management**

|  |  |
| --- | --- |
|  | **TSP-13: Insurance Management** |
| **Описание** | Эта мера использует страхование для передачи риска третьему лицу в обмен на уплату фиксированного сбора или премии. |
| **Ценность/значение** | Финансовые последствия серьезных инцидентов можно смягчить, разделив риск с другими участниками посредством заключения соответствующего страхового полиса. |
| **Входные данные** | * Отчет об угрозах страхования (GP-3); * Инвентаризация основных средств (OSP-3). |
| **Выходные данные** | * Угрозы Застрахованы; * Договоры страхования (ОСП-15); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**TSP-7: Background Checks (проверка биографии)**

|  |  |
| --- | --- |
|  | **TSP-7: Background Checks** |
| **Описание** | Этот процесс направлен на обеспечение того, чтобы новые сотрудники, выполняющие ответственные роли, не представляли угрозы для организации. |
| **Ценность/значение** | Персонал, которому доверяют осуществлять процессы обеспечения безопасности, должен быть компетентным, подотчетным и наделенным полномочиями. |
| **Входные данные** | * Определение должности (из отдела кадров); * Кадровая политика (от Human Resources). |
| **Выходные данные** | * Отчет о проверке биографических данных (положительный или отрицательный) (для людских ресурсов); * Подписано соглашение о неразглашении информации; * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**TSP-9: Security Personnel Training**

|  |  |
| --- | --- |
|  | **TSP-9: Security Personnel Training** |
| **Описание** | Этот процесс гарантирует, что сотрудники Службы безопасности развивают свои навыки и профессиональные навыки. |
| **Ценность/значение** | Персонал, которому доверяют осуществлять процессы обеспечения безопасности, должен быть компетентным, подотчетным и наделенным полномочиями. Запланированная и контролируемая программа обучения и развития необходима для обеспечения того, чтобы процессы выполнялись компетентным персоналом. |
| **Входные данные** | * Кадровая политика (от Human Resources). |
| **Выходные данные** | * Обучение по докладу о безопасности (для людских ресурсов); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**TSP-14: Information Operations**

|  |  |
| --- | --- |
|  | **TSP-14: Information Operations** |
| **Описание** | Этот процесс собирает информацию о возможностях потенциальных и нынешних злоумышленников, дезинформируя их о сильных и слабых сторонах организации. |
| **Ценность/значение** | Чем менее точной и полной информацией обладает потенциальный злоумышленник об организации, тем меньше вероятность того, что атака будет успешной, и тем выше будет стоимость любой такой атаки. Чем более полной и точной информацией организация располагает о потенциальных злоумышленниках, тем больше вероятность того, что организация сможет защититься от атак. |
| **Входные данные** | * GP-024: политика информационной безопасности * TSP-143: процедура дезинформации; * TSP-144: процедура шпионажа потенциальных злоумышленников; * TSP-145: процедура контрразведки потенциальных злоумышленников. |
| **Выходные данные** | * Дезинформационный отчет (TSP-4); * Отчет о возможностях потенциальных злоумышленников (GP-3); * Потенциальным злоумышленникам доклад о Контршпионаже (GP-3); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**Операционные процессы**

Оперативное руководство подчиняется главному информационному директору и тактическому менеджеру по информационной безопасности.

Оперативное управление имеет следующие конкретные цели и обязанности:

* Предоставление обратной связи тактическому руководству, включая отчеты об инцидентах и показателях;
* Эффективно и результативно использовать выделенные ресурсы;
* Идентификация и защита активов в рамках жизненного цикла;
* Защита и поддержка информационных систем на протяжении всего их жизненного цикла;
* Применение управления доступом и экологического контроля для пользователей и служб;
* Управление доступностью (может совместно использоваться с управлением доступностью ИТ-операций и Управлением непрерывностью ИТ-услуг);
* Тестирование и аудит;
* Мониторинг и управление жизненным циклом мер безопасности;
* Выполнение процессов предотвращения, обнаружения и смягчения последствий инцидентов (как в режиме реального времени, так и  
  после инцидента).

**OSP-1: Report to Tactical Management**

|  |  |
| --- | --- |
|  | **OSP-1: Report to Tactical Management** |
| **Описание** | Регулярный отчет о результатах процесса и использовании выделенных ресурсов. |
| **Ценность/значение** | Отчет тактическому руководству необходим для того, чтобы показать эффективность и результативность конкретных используемых процессов. |
| **Входные данные** | * Отчеты по метрикам из операционных процессов (такие же, как для TSP-4). |
| **Выходные данные** | * Отчет о безопасности оперативной информации (TSP-1, TSP-4). |
| **Метрические описания** | N/A |

**OSP-2: Security Procurement**

|  |  |
| --- | --- |
|  | **OSP-2: Security Procurement** |
| **Описание** | Выбор конкретных продуктов, поставщиков и поставщиков аутсорсинга, которые наилучшим образом соответствуют целям и показателям информационной безопасности в рамках выделенного бюджета. |
| **Ценность/значение** | Эффективное использование ресурсов является результатом эффективного выбора соответствующих инструментов безопасности, поставщиков и аутсорсинговых услуг. |
| **Входные данные** | * Отчеты о самооценке поставщиков Иерихонского форума; * Табло безопасности и рейтинги пользователей; * Критерии отбора лучшие практики (обновления, метрики, кривая обучения и т. д.); * Цели информационной безопасности (TSP-3); * Бюджет информационной безопасности (SSP-6). |
| **Выходные данные** | * Отчет о рекомендациях по закупкам (GP-3); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**Управление Жизненным Циклом**

Поддержание жизненного цикла обычно входит в обязанности отдела информационных систем. Роль безопасности несет ответственность за защиту информационных систем на протяжении всего их жизненного цикла.

**OSP-3: Inventory Management**

|  |  |
| --- | --- |
|  | **OSP-3: Inventory Management** |
| **Описание** | Этот процесс определяет, оценивает и оценивает активы (репозитории, интерфейсы, службы и каналы), подлежащие защите. Он должен идентифицировать:   * Владелец информационной системы для каждой информационной системы, управляемый ею домен, к которому она принадлежит, и текущее состояние в пределах этого управляемого домена; * Уполномоченная аудитория важных съемных хранилищ ведет инвентаризацию копий, и кто ими владеет; * Лицензирование установленного и деинсталлированного программного обеспечения.   Лицензирование используемой информации, защищенной авторским правом. Ведение полностью точной инвентаризации может быть дорогостоящим и чрезвычайно трудным в крупных организациях. O-ISM3 распознает эту трудность, поэтому этот процесс может выполняться либо как периодический, либо как процесс обнаружения в реальном времени. |
| **Ценность/значение** | Функционирование ISM зависит от идентификации критически важных активов для защиты и соответствующей классификации с использованием, например, языка разметки обеспечения информации (IAML). |
| **Входные данные** | * Известное оборудование; * Известное программное обеспечение; * Другие известные информационные хранилища; * Классификация систем и приложений; * Инвентаризация систем и приложений; * Отчет о клиринге (OSP-6). |
| **Выходные данные** | * Инвентаризация активов (несколько процессов); * Секретные хранилища и сообщения; * Приоритетные интерфейсы, службы и каналы; * Долговечность и качество сгруппированных хранилищ; * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**OSP-5: IT Managed Domain Patching**

|  |  |
| --- | --- |
|  | **OSP-5: IT Managed Domain Patching** |
| **Описание** | Этот процесс охватывает постоянное обновление служб для предотвращения инцидентов, связанных с известными слабостями, повышения надежности обновляемых систем. |
| **Ценность/значение** | Исправление ошибок предотвращает инциденты, возникающие в результате использования известных слабых мест в службах. |
| **Входные данные** | * Инвентаризация основных средств (ОСП-3). |
| **Выходные данные** | * Современные сервисы в каждом управляемом ИТ-домене; * Отчет об уровне обновления служб (OSP-4); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | Уровень обновления, рассчитываемый следующим образом:   * Уровень обновления для конкретной информационной системы равен сумме дней, оставшихся для всех ожидающих исправлений безопасности; * Уровень обновления управляемого ИТ-домена равен сумме отдельных уровней обновления, деленной на количество информационных систем.   Чем ниже этот показатель, тем лучше. Эта метрика позволяет проверить ход процесса исправления и сравнить уровень обновления различных управляемых ИТ-доменами доменов.  Также метрика, используемая для описания – **Activity** (Большая активность => более высокий уровень возможности процесса => более высокий уровень ИБ) |

**OSP-7: IT Managed Domain Hardening**

|  |  |
| --- | --- |
|  | **OSP-7: IT Managed Domain Hardening** |
| **Описание** | Этот процесс улучшает конфигурацию каналов, служб, портов, интерфейсов и хранилищ, повышая их надежность. Этот процесс удаляет неиспользуемые каналы, службы, порты, интерфейсы и репозитории. |
| **Ценность/значение** | Усиление управляемого домена ИТ требуется для активов, особенно на границах управляемого домена ИТ, где активы видны зонам с более низкой или неизвестной безопасностью. Это делается для защиты информации в видимой зоне и предотвращения распространения видимой зоны дальше, чем требуется внутри организации. |
| **Входные данные** | * Инвентаризация основных средств (OSP-3). |
| **Выходные данные** | * Улучшенные сервисы, интерфейсы, репозитории и каналы; * Отчет о закаливании (ОСП-4); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | Уровень обновления, рассчитываемый следующим образом:   * Уровень обновления для конкретной информационной системы равен сумме дней, оставшихся для всех ожидающих исправлений безопасности; * Уровень обновления управляемого ИТ-домена равен сумме отдельных уровней обновления, деленной на количество информационных систем.   Чем ниже этот показатель, тем лучше. Эта метрика позволяет проверить ход процесса упрочнения и сравнить уровень упрочнения различных управляемых ею областей. |

**OSP-16: Segmentation and Filtering Management**

|  |  |
| --- | --- |
|  | **OSP-16: Segmentation and Filtering Management** |
| **Описание** | Этот процесс определяет техническую политику для прохождения разрешенных сообщений и электромагнитных волн между зонами, одновременно запрещая проход несанкционированным сообщениям и электромагнитным волнам. Сообщения и ЭМ волны могут быть отфильтрованы на любом уровне абстракции, начиная от брандмауэров уровня 7 до фильтрации спама, фильтрации мгновенных сообщений, фильтрации трафика TCP/IP, фильтрации VoIP, фильтрации электромагнитных импульсов и т. д. |
| **Ценность/значение** | Инциденты, возникающие в результате вторжения, вандализма и неправильного использования информационных систем, могут быть предотвращены и смягчены путем соответствующей сегментации управляемых ИТ-доменами и хранилищами и фильтрации сообщений. |
| **Входные данные** | * Определение управляемых доменов и жизненных циклов; * Инвентаризация основных средств (ОSP-3); * Отчет об обнаружении инцидента (OSP-23); * Отчет об обнаружении вторжений (OSP-23). |
| **Выходные данные** | * Предотвращение несанкционированного прохождения сообщений между управляемыми им доменами * Отчет о правилах фильтрации (TSP-4); * Журналы отбросов (почты, пакетов, веб-посещений и т. д.) (ОSP-23); * Журналы пропусков (почты, пакетов, веб-посещений и т. д.) (ОSP-23); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | Уровень обновления, рассчитываемый следующим образом:   * Уровень обновления каждой фильтрующей системы равен количеству дней, прошедших с момента уведомления об обновлениях, но еще не примененных; * Общий уровень обновления равен сумме отдельных уровней обновления, деленной на количество фильтрующих систем.   Чем ниже этот показатель, тем лучше. Эта метрика обеспечивает проверку уместности текущих механизмов фильтрации и позволяет сравнивать уровень обновления различных управляемых ИТ-доменов. |

**OSP-17: Malware Protection Management**

|  |  |
| --- | --- |
|  | **OSP-17: Malware Protection Management** |
| **Описание** | Это комплекс мер безопасности для обеспечения защиты от технических угроз, таких как вирусы, шпионские программы, трояны, бэкдоры, регистраторы ключей, руткиты и другие несанкционированные сервисы. Альтернативой очистке или удалению несанкционированной службы является помещение ее в изолированную “песочницу”. |
| **Ценность/значение** | Инциденты, связанные с заражением внутренних ресурсов вредоносными программами, могут быть предотвращены и смягчены соответствующим процессом защиты от вредоносных программ. |
| **Входные данные** | * Инвентаризация основных средств (ОSP-3); * Отчет об обнаружении инцидента (OSP-23). |
| **Выходные данные** | * Защита информационных систем от вредоносных программ; * Отчет об обнаружении и очистке вредоносных программ (OSP-23); * Отчет об уровне развертывания и обновления защиты от вредоносных программ (TSP-4); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | Уровень обновления, рассчитываемый следующим образом:   * Уровень обновления вредоносных программ для каждой информационной системы равен количеству дней, прошедших с момента уведомления об обновлениях сигнатур вредоносных программ, но еще не примененных; * Общий уровень обновления вредоносных программ управляемого домена равен сумме отдельных уровней обновления вредоносных программ, деленной на количество информационных систем.   Чем ниже этот показатель, тем лучше. Этот показатель измеряет степень готовности к новым вредоносным программам и позволяет сравнить уровень обновления различных управляемых ИТ-доменов. |

**Доступ и экологический контроль**

**OSP-11: Access Control**

|  |  |
| --- | --- |
|  | **OSP-19: Internal Technical Audit** |
| **Описание** | Контроль доступа - это средство, с помощью которого доступ к секретной информации предоставляется авторизованным пользователям и запрещен несанкционированным. Контроль доступа включает в себя аутентификацию пользователей или служб, авторизацию пользователей или служб, подписание репозиториев и запись доступа и использования сервисов, репозиториев, каналов и интерфейсов. |
| **Ценность/значение** | Чтобы сделать пользователей ответственными за использование сервисов, интерфейсов и доступ к репозиториям, необходимо связать использование учетных записей пользователей с их владельцем, предоставить или запретить доступ к сервисам, интерфейсам и репозиториям в режиме реального времени и записать его. |
| **Входные данные** | * Инвентаризация основных средств (ОSP-3); * Инвентаризация помещений (от объектов); * Отчет о проверке регистрации пользователей и контроля доступа (OSP-19). |
| **Выходные данные** | * Предоставление доступа авторизованным пользователям; * Отказ в доступе к неавторизованным пользователям; * Журналы доступа к секретным репозиториям; * Журналы доступа к засекреченным помещениям; * Журналы использования классифицированных сервисов и интерфейсов; * Отчет о попытках несанкционированного доступа (TSP-4). |
| **Метрические описания** | * Процент учетных записей пользователей с настроенными задержками между последовательными неудачными входами в систему; * Процент учетных записей пользователей, для которых истекает срок действия сеансов; * Процент учетных записей пользователей, для которых максимальное количество одновременных сеансов равно одному; * Процент учетных записей пользователей, для которых истекает срок действия учетных данных; * Процент учетных записей пользователей, для которых контролируется качество учетных данных пароля. |

**Контроль Доступности**

**OSP-27: Archiving Management**

|  |  |
| --- | --- |
|  | **OSP-27: Archiving Management** |
| **Описание** | Это комплекс мер безопасности, обеспечивающих долговременную доступность хранимой информации в ситуациях, установленных требованиями к длительным срокам хранения. Стратегии, гарантирующие возможность извлечения информации, включают копирование информации со старых носителей и форматов на текущие или поддержание устаревших систем в рабочем состоянии и мониторинг качества носителей информации. |
| **Ценность/значение** | Инциденты, возникающие в результате потери хранилищ до определенного срока хранения или хранения их после истечения срока годности, могут быть смягчены хранением, каталогизацией и периодическим мониторингом возможности извлечения. |
| **Входные данные** | * Инвентаризация основных средств (ОSP-3). |
| **Выходные данные** | * Предотвращение постоянной потери информации из хранилищ; * Отчет об архивном хранении (ОСП-15); * Отчет о восстановлении архива (OSP-15); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | Доля физических хранилищ старше конца срока службы. |

**Тестирование и аудит**

Процесс: **OSP-19: Internal Technical Audit**

|  |  |
| --- | --- |
|  | **OSP-19: Internal Technical Audit** |
| **Описание** | Этот процесс проверяет правильность:   * Эффективность мер по снижению уязвимости; * Эффективность мер контроля доступа; * Эффективность мер по регистрации пользователей; * Эффективность фильтрующих мероприятий; * Качество программного обеспечения, разработанного собственными силами. Он может быть применен ко всем возможным целям или репрезентативной случайной выборке.   При выполнении эмулированных атак из внутренних систем это обычно называют внутренним тестированием "уязвимости". При выполнении эмулируемых атак из внешних систем, обычно известен как "тестирование на проникновение". |
| **Ценность/значение** | Инциденты, возникающие в результате использования уязвимых мест в программном обеспечении и конфигурации слабых мест вокруг границ организации, могут быть предотвращены эмуляцией атак и последующей починкой программного обеспечения, укреплением управляемого ИТ-доменом домена, инвестициями и улучшенным мониторингом. |
| **Входные данные** | Инвентаризация основных средств (OSP-3) |
| **Выходные данные** | * Отчет об эмуляции атаки (OSP-4); * Отчет о проверке исходного кода (OSP-8); * Отчет о проверке регистрации пользователей и контроля доступа (OSP-12, OSP-11); * Отчет о мерах фильтрации (TSP-4); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | * Доля обнаруженных уязвимостей, которые являются ложными негативами; * Доля существующих уязвимостей, которые не найдены.   Чем выше доля обнаруженных и вовремя исправленных уязвимостей, тем выше будет уровень информационной безопасности.  Чем ниже доля необнаруженных уязвимостей, тем выше будет уровень информационной безопасности.  Метрики: Quality, Effectiveness, Activity (больше аудитов-выше уровень безопасности). |

**Мониторинг**

**OSP-22: Alerts Monitoring**

|  |  |
| --- | --- |
|  | **OSP-22: Alerts Monitoring** |
| **Описание** | Этот процесс проверяет, что ISM осведомлена о новых угрозах, создаваемых третьими сторонами, угрозах для третьих сторон, исходящих от организации, слабых местах и исправлениях, и позволяет принимать обоснованные решения о том, следует ли изменять конфигурацию информационной системы или уровень исправлений, или даже эволюцию системы управления. Как сотрудники, так и третьи лица могут внести свой вклад в выявление слабых мест. |
| **Ценность/значение** | Инциденты, возникающие в результате использования опубликованных слабых мест в продуктах и программном обеспечении, могут быть предотвращены своевременным применением соответствующих корректирующих мер.  Слабые места в производственных системах, обнаруженные сотрудниками или третьими лицами, нуждаются в корректирующих действиях.  Новые угрозы могут потребовать внесения изменений в ISM. |
| **Входные данные** | * Отчеты о слабостях, исправлениях и угрозах (из внешних и внутренних источников); * Инвентаризация основных средств (ОSP-3). |
| **Выходные данные** | * Просмотр предупреждений, исправлений и отчетов о слабостях; * Отчет о предупреждениях, исправлениях и угрозах (OSP-4); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | * Доля предупреждений, которые ошибочно считаются нерелевантными (ложноотрицательными); * Доля предупреждений, которые неправильно считаются релевантными (ложноположительными). |

**Обработка инцидентов**

**OSP-24: Handing of Incidents and Near-incidents**

|  |  |
| --- | --- |
|  | **OSP-22: Alerts Monitoring** |
| **Описание** | Этот процесс направлен на ограничение воздействия инцидентов и сбор информации. Цели управления инцидентами заключаются в следующем:   * Содержать последствия инцидента, не включая восстановление хранилищ и информационных систем, за которое отвечают OSP-10, OSP-15 и OSP-26; * Сбор данных для судебно-медицинской экспертизы; * Соберите информацию, чтобы извлечь уроки из инцидента; * Сбор данных для оценки воздействия и эффективности инвестиций в безопасность.   Мошенничество-это очень важный тип инцидента. Альтернативное название этого процесса - **OSP-24: Fraud Handling**, который рекомендуется для конкретных реализаций мошенничества. |
| **Ценность/значение** | Четкие процедуры обработки инцидентов могут помочь смягчить последствия инцидента и предотвратить его повторение в будущем. Информация об инцидентах, вторжениях и атаках должна использоваться для улучшения функционирования мер безопасности, принятия решений об инвестициях в безопасность оценки эффективности мер безопасности. |
| **Входные данные** | * Отчет об обнаружении инцидента (OSP-23); * Отчет об обнаружении вторжений (OSP-23). |
| **Выходные данные** | * Обработанные инциденты и почти инциденты; * Отчет об инциденте (OSP-25, TCP-10); * Отчет о вторжении (OSP-25); * Отчет по метрикам (TSP-4). |
| **Метрические описания** | N/A |

**Вывод**

Модель ISM3 является инструментом разработки, отвечающей бизнес-целям организации, и постоянного мониторинга ее исполнения. При этом модель совместима со всеми основными стандартами и методологиями, например, ISO 9001, ISO/IEC 27001 и ISO/IEC 27002, CobIT, ITIL и т.д. Поэтому ISM3 может использоваться для внедрения СУИБ с последующей ее сертификацией по ISO/IEC 27001 и 27002.

Преимущество O-ISM3 – то, что этот стандарт полностью основан на процессном подходе к управлению ИБ и его зрелости: каждое средство управления ИБ нуждается в управляющем им процессе. Это разбивает управление ИБ на большое, но управляемое число процессов, с соответствующими средствами управления, определенными внутри каждого процесса как необходимые его подмножества.

В отличие от других подобных стандартов, в которых большое внимание уделяется функциям средств управления, стандарт O-ISM3 описывает основные процессы управления ИБ, присущие большинству организаций. Выделяются задачи процессов ОИБ и метрики, непосредственно вытекающие из бизнес-целей организации. Отмечается, что каждый процесс ОИБ вносит свой вклад в реализацию основных целей управления ИБ, которые определяются следующим образом:

* Предотвращать и снижать число инцидентов ИБ, которые могут поставить под угрозу активы организации, поставляемую ею продукцию и предоставляемые сервисы, основанные на использовании информационных систем;
* Оптимизировать использование информации, финансов, людей, времени и инфраструктуры.