Обзор процессов для построения кибербезопасности в организации

Автор:
Пономарев Артемий

Старший специалист группы
методологии управления ИБ

Оглавление

1. Введение

В настоящее время не существует стандарта, описывающего процессы ИБ в организации, поэтому каждая организация строит систему обеспечения ИБ, основываясь на своем представлении о целевой картине.

Для IT существуют фреймворки, которые описывают процессы (практики), необходимые для построения эффективной системы управления IT. В информационной безопасности существует только стандарт ISO/IEC 27001, который устанавливает требования к тому, что необходимо сделать (или делать) для построения системы управления информационной безопасностью. При этом в данном стандарте не поясняется, какие конкретно процессы следует реализовать и каким образом.

В настоящей статье предлагается фреймворк процессной модели ИБ, при помощи которой можно взглянуть на картину процессов, обеспечивающих ИБ в организациях, целиком. При создании фреймворка процессной модели ИБ сначала рассматривается архитектура организации с различных перспектив, затем анализируется IT-фреймворк COBIT 5; далее, т. к. ИБ предъявляет более широкие требования, чем IT, рассматриваются другие процессы, необходимые для обеспечения ИБ. Фреймворк процессной модели представлен в виде карты процессов, составленной на основе наиболее необходимых процессов ИБ организации.

2. Архитектура организации с различных перспектив

Архитектура организации может иметь разное представление в зависимости от положения наблюдателя в организационной структуре компании. Архитектура организации с позиций (перспектив) руководства организации, IT и ИБ представлена на рис. 1.

Рисунок 1. Различные перспективы архитектуры организации.

Из рис. 1 видно, что архитектура организации со стороны различных подразделений и руководства выглядит по-разному. При этом нужно понимать, что функции IT и ИБ строятся на основе бизнес-процессов, а некоторые процессы ИБ могут предоставляться в виде IT-сервиса.

Вся деятельность организации может быть показана с точки зрения осуществляемых бизнес-процессов. При этом сами бизнес-процессы могут быть представлены на различных уровнях детализации (например, вся функция IT определяется в виде одного блока на общей карте процессов — модели из 37 процессов по COBIT 5).

Обсуждение процессов, необходимых для поддержания высокого уровня кибербезопасности, невозможно без рассмотрения других связанных с обеспечением ИБ процессов, таких как IT-процессы, процессы управления персоналом, процессы физической безопасности, юридическая поддержка деятельности организации, управление корпоративными рисками.

[1] По мнению автора, не является частью модели COBIT 5.

3. Архитектура организации с различных перспектив

3.1 IT-процессы организации

Рассмотрим IT-процессы организации, ориентируясь на модель COBIT 5, содержащую 37 процессов (COBIT 5 используем как наиболее подходящую). В каждом процессе модели можно определить цели процесса, относящиеся к безопасности (например, COBIT 5 для информационной безопасности). На рис. 2 показана модель процессов COBIT 5. Отдельно показаны наиболее сильные связи процессов эталонной модели COBIT 5 с функцией информационной безопасности[1] . Эталонная модель COBIT 5 дает представление о структуре зрелых процессов IT в организациях; ее полезно рассмотреть для понимания процессов функции IT-службы.

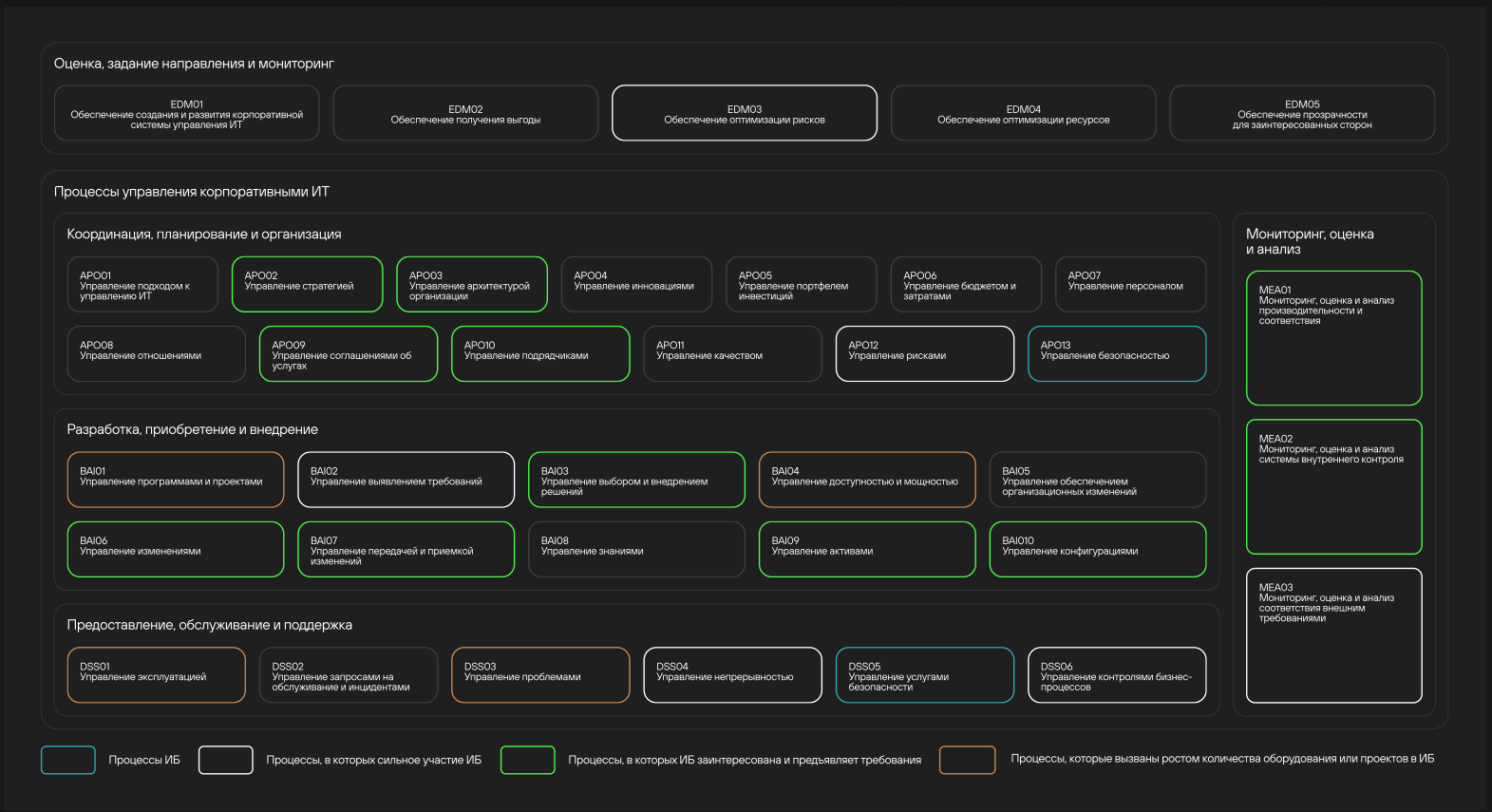

Рисунок 2. Эталонная модель процессов по COBIT 5 с анализом влияния ИБ

3.1.1 Процессы ИБ в COBIT 5

Напрямую к функции ИБ относятся только процессы DSS05 и APO13. Эти процессы осуществляются функцией ИБ.

Функция ИБ — сотрудник или подразделение, отвечающее за реализацию процессов ИБ в организации.

[1] По мнению автора, не является частью модели COBIT 5.

APO13 Управление безопасностью

Процесс, непосредственно показывающий функцию ИБ и состоящий из построения и поддержания системы менеджмента ИБ, определения рисков ИБ, управления рисками ИБ и планом их обработки, мониторинга и пересмотра системы менеджмента ИБ.

DSS05 Управление услугами безопасности

Современные IT-фреймворки построены по сервисной модели, поэтому функции ИБ тоже показаны как услуги безопасности. Данный блок состоит из антивирусной защиты, управления сетевой безопасностью, управления безопасностью конечных точек, управления доступом и идентификаторами пользователей, управления физическим доступом к IT-активам, управления документами ограниченного доступа, мониторинга событий информационной безопасности.

3.1.2 Процессы с сильным влиянием ИБ

Процессы с наибольшим влиянием функции ИБ обычно осуществляются совместно с заинтересованными сторонами или полностью передаются в функцию ИБ.

EDM03 Обеспечение оптимизации рисков

На уровне руководства организации должны быть установлены общие параметры по риск-аппетиту и толерантности к риску. Эти параметры используются для управления рисками организации. Риск-аппетит и толерантность к риску должны быть установлены и для рисков ИБ, которые всегда рассматриваются при построении общей системы управления рисками организации. Риски ИБ должны рассматриваться на уровне руководства организации. Риски IT и ИБ обычно объединяются в единый профиль риска, который постоянно отслеживается в соответствии с требованиями ERM. Профиль риска ИБ обычно содержит ключевые риск-факторы, которые можно представить как недопустимые события.

APO12 Управление рисками

Полученные параметры используются на операционном уровне для построения системы оценки рисков ИБ. Риски организации могут оцениваться в различных сферах по-разному. Риски в области охраны труда или экологического менеджмента оцениваются по своим методикам, а риски IT и ИБ — по своим. Например, такой инцидент, как падение сервера на ногу работнику, будет интересен функции ИБ с точки зрения потери данных, а службе охраны труда — с точки зрения серьезности нанесенной травмы. Риски ИБ обычно составляют львиную долю рисков IT и ИБ.

BAI02 Управление выявлением требований

Требования ИБ должны формулироваться и предъявляться к IT-решениям перед их приобретением или созданием. Требования ИБ предъявляются на уровне законодательства и должны быть учтены практически в любой информационной системе организации на стадии проектирования. Чем раньше предъявляются и учитываются требования ИБ к информационной системе, тем меньше потом приходится переделывать.

DSS04 Управление непрерывностью

Ни для кого не секрет, что инциденты ИБ могут стать причиной остановки бизнеса. Поэтому для случая их наступления должны разрабатываться планы восстановления и планы непрерывности бизнеса. Например, если в организации не предусмотрен план восстановления основных информационных систем, то даже простой вирус-шифровальщик может остановить бизнес-процесс на долгое время (возможно навсегда).

DSS06 Управление контролями бизнес-процессов

Функция ИБ ответственна за определение требований к управлению информацией и применение адекватных мер ее защиты для обеспечения соответствия самой информации и применимых методов обработки информации требованиям информационной безопасности. Требования ИБ предъявляются как к автоматизированным частям бизнес-процесса, так и неавтоматизированным, и поэтому являются более широкими в сравнении с требованиями функции IT.

MEA03 Мониторинг, оценка и анализ соответствия внешним требованиями

Внешние требования к IT должны регулярно отслеживаться. Законодательные требования к информационной безопасности IT предъявляются в основном для обеспечения должного уровня информационной безопасности. Поэтому функция ИБ обычно отслеживает изменения в законодательстве и совместно с функцией IT разрабатывает мероприятия по приведению IT в соответствие требованиям. Также могут быть поставлены задачи на соответствие стандартам информационной безопасности, например ISO/IEC 27001:2022 «Системы менеджмента информационной безопасности. Требования».

3.1.3 Процессы IT, в исполнении которых функция ИБ заинтересована

Процессы, в которых функция ИБ заинтересована и предъявляет к ним требования.

APO02 Управление стратегией

Трудно представить развитие IT без должного внимания к ИБ. Поэтому вопросы ИБ всегда учитываются при построении IT стратегии.

APO03 Управление архитектурой организации

Требования ИБ должны быть учтены при построении IT-архитектуры организации.

APO09 Управление соглашениями об услугах

К некоторым IT-услугам должны быть предъявлены SLA по информационной безопасности. Функция ИБ также может осуществлять свою деятельность в форме услуг ИБ.

APO10 Управление подрядчиками

К подрядчикам обычно предъявляются требования ИБ. Они связаны с неразглашением информации и с выполнением требований ИБ при работе в IT-инфраструктуре организации.

BAI03 Управление выбором и внедрением решений

Одним из критериев выбора решений является их информационная безопасность. Поэтому функция ИБ должна исполнять свою роль в предъявлении требований и оценке выбираемых IT решений.

BAI06 Управление изменениями

Требования ИБ должны учитываться при оценке влияния изменений в приложениях и IT-инфраструктуре. Подробнее о контроле изменений в IT можно прочитать в статье «Рекомендации по контролю изменений в IT-инфраструктуре».

BAI07 Управление передачей и приемкой изменений

Тестирование ИБ должно являться неотъемлемой частью приемочных испытаний для некоторых видов изменений. Особенно в тех случаях, когда вводится новый функционал или изменяется прежний функционал средств обеспечения ИБ.

BAI09 Управление активами

Все приобретенные IT-активы должны отвечать требованиям ИБ. Для каждого актива должны быть определены ответственные лица (владельцы актива). В организации должны функционировать средства ИБ, предотвращающие использование устройств, подключенных несанкционированно.

BAI010 Управление конфигурациями

В отличие от предыдущего процесса, данный процесс управляет информацией о связях между IT-активами и необходимыми конфигурациями IT-активов. Может использоваться функцией ИБ для понимания связей между IT-активами и для предъявления требований к конфигурации IT-активов.

MEA01 Мониторинг, оценка и анализ производительности и соответствия

Функция ИБ предъявляет требования к организации журналирования событий в информационных системах и настройке отправки журналов событий на выделенные средства защиты информации (например, SIEM-система) для их дальнейшего анализа на предмет выявления инцидентов ИБ. Используемые средства защиты информации также должны подвергаться мониторингу соответствия их производительности выполняемым задачам.

MEA02 Мониторинг, оценка и анализ системы внутреннего контроля

Функция ИБ в основном является функцией контроля в отношении функции IT организации. IT-функция должна обеспечить открытость в отношении своей деятельности для проведения контрольных мероприятий со стороны функции ИБ. Установленные меры контроля со стороны функции ИБ должны быть под постоянным мониторингом, обеспечивающим гарантию их эффективности.

MEA01 Мониторинг, оценка и анализ производительности и соответствия

Функция ИБ предъявляет требования к организации журналирования событий в информационных системах и настройке отправки журналов событий на выделенные средства защиты информации (например, SIEM-система) для их дальнейшего анализа на предмет выявления инцидентов ИБ. Используемые средства защиты информации также должны подвергаться мониторингу соответствия их производительности выполняемым задачам.

MEA02 Мониторинг, оценка и анализ системы внутреннего контроля

Функция ИБ в основном является функцией контроля в отношении функции IT организации. IT-функция должна обеспечить открытость в отношении своей деятельности для проведения контрольных мероприятий со стороны функции ИБ. Установленные меры контроля со стороны функции ИБ должны быть под постоянным мониторингом, обеспечивающим гарантию их эффективности.

3.1.4 Процессы ИБ, связанные с объемом функции ИБ

Если функция ИБ большая, то возможно управлять процессами ИБ как IT-процессами. В большинстве случаев оптимально использовать процессы функции IT, распространив их на функцию ИБ. Но если IT-процессов нет, то необходимо выстраивать свои процессы.

BAI01 Управление программами и проектами

Соответствующий процесс появляется при большом объеме проектов ИБ, которыми необходимо управлять

BAI04 Управление доступностью и мощностью

Функция ИБ должна контролировать мощности используемых средств защиты информации и управлять этими мощностями. Требования к возможной нагрузке на СЗИ должны учитывать развитие IT и организации в целом.

DSS01 Управление эксплуатацией

При появлении сложных СЗИ возникают вопросы построения процесса их эксплуатации.

DSS03 Управление проблемами

В ходе эксплуатации большого парка СЗИ возникает потребность не только в закрытии инцидентов с его функционированием, но и в решении проблем, возникающих при эксплуатации.

3.2 HR-процессы организации

HR-процессы включают в себя процессы рекрутинга, управления мотивацией и квалификацией персонала, создания корпоративной культуры. Они существуют во всех HR-отделах и не зависят от масштаба или типа организации напрямую.

Приведем основные функции информационной безопасности, относящиеся к HR-процессам в соответствии с Приложением стандарта ISO/IEC 27001:2022 (на момент написания не переведен на русский язык). Данному вопросу посвящен раздел A.6 People controls (контроль персонала). В таблице ниже приведены требования стандарта с маппингом на процессы HR.

№ п	Требование приложения стандарта	Соответствующий условный HR-процесс	Пояснение
A. 6.1	Предварительная проверка	Рекрутинг	Проверка кандидатов при приеме на работу
A. 6.2	Условия трудового соглашения	Рекрутинг	Трудовые соглашения должны устанавливать взаимную ответственность в части информационной безопасности
A. 6.3	Осведомленность, образование и подготовка в сфере информационной безопасности	Управление квалификацией персонала	Работники должны быть осведомлены о требованиях информационной безопасности в соответствии с занимаемой должностью (ролью)
A. 6.4	Дисциплинарный процесс	Привлечение работника к дисциплинарной ответственности	В отношении нарушивших требования ИБ работников должны приниматься меры дисциплинарного взыскания
A. 6.5	Ответственность после прекращения или изменения трудовых отношений	Прекращение или изменение трудовых отношений	Трудовые соглашения должны устанавливать ответственность и обязанности по соблюдению информационной безопасности, которые остаются в силе после прекращения или изменения трудовых отношений
A. 6.6	Соглашения о конфиденциальности или неразглашении	Рекрутинг	Соглашения о конфиденциальности или неразглашении должны быть актуальными и подписанными персоналом
A. 6.7	Удаленная работа	В рамках стандартного процесса рекрутинга	В связи с удаленной работой персонала должны быть предусмотрены дополнительные меры защиты
A. 6.8	Отчетность о событиях информационной безопасности	Управление квалификацией персонала	Персонал должен быть осведомлен о способах информирования об инциденте ИБ или о подозрении на инцидент

3.3 Физическая охрана IT-активов

Без обеспечения физической охраны IT-активов сложно говорить о кибербезопасности. Например, в случае получения злоумышленником прямого доступа к серверам компании он как минимум может нанести ущерб доступности и целостности информации (если информация зашифрована). Поэтому IT-активы должны быть защищены не только внутри организации, но и за ее пределами, сотрудники должны быть осведомлены об основных обязанностях по обеспечению безопасности IT-активов, а технические меры защиты должны предусматривать возможную кражу IT-активов (например, для защиты телефонов используются MDM-решения, позволяющие удаленно контролировать данные).

3.4 Юридическая поддержка

Нередко функции ИБ требуется юридическая поддержка со стороны соответствующих подразделений организаций. Это может быть и договорная работа, и юридическое преследование внутренних и внешних злоумышленников, и получение консультаций по изменениям в законодательстве.

3.5 Корпоративная система управления рисками

В зрелых организациях функционирует корпоративная система управления рисками. Функция ИБ должна синхронизировать свои активности в части анализа рисков ИБ с общей корпоративной системой управления рисками. Эта активность связана с процессом «EDM03 Обеспечение оптимизации рисков».

3.6 Непрерывность деятельности

Внедрение системы управления непрерывностью деятельности должно сопровождаться выполнением требований ИБ. При разработке планов обеспечения непрерывности деятельности должны учитываться требования по сохранению установленного уровня информационной безопасности.

4. Фреймворк процессной модели ИБ

На основании анализа процессов, необходимых для поддержания высокого уровня киберустойчивости, составим фреймворк процессной модели, который представим в виде карты процессов и их описания. На рис. 3 приведена карта, включающая основные процессы, необходимые для построения системы с высоким уровнем киберустойчивости. Процессы исполняются различными функциональными подразделениями организации — в основном это функции IT и ИБ организации.

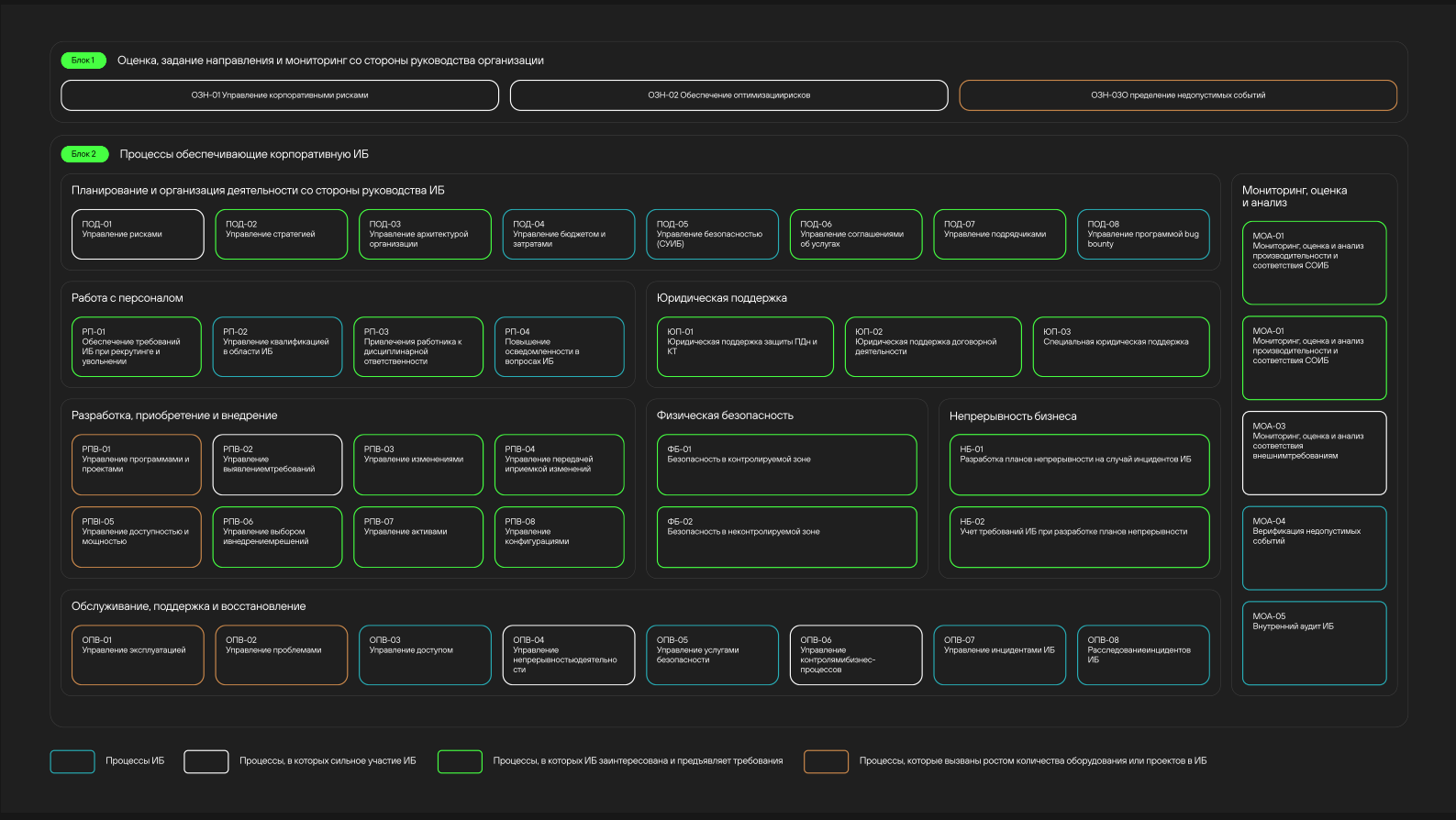

Рисунок 3. Эталонная модель процессов корпоративной ИБ

Карта состоит из двух блоков.

Блок оценки, задания направления и мониторинга со стороны руководства организации ИБ отвечает за поддержание процессов ИБ со стороны руководства. Поддержка со стороны руководства организации является обязательным условием внедрения результативной кибербезопасности.

Данный блок состоит из трех процессов:

- Управление корпоративными рисками (ОЗН-01);
- Обеспечение оптимизации рисков (ОЗН-02);
- Определение недопустимых событий (ОЗН-03).

Описание данного блока процессов приведено ниже.

Наименование процесса	Описание процесса
Управление корпоративными рисками (ОЗН-01)	Все организации имеют разные стратегии в области управления рисками: одни готовы идти на риск ради получения выгоды, другие — нет. Все понимают, что это имеет существенное влияние на принимаемые решения, в том числе в области кибербезопасности. В корпоративной системе управления рисками должны быть установлены основные параметры управления корпоративными рисками (риск-аппетит и толерантность к риску)
Обеспечение оптимизации рисков (ОЗН-02)	Для своевременного управления рисками ИБ необходимо установить понятный подход к управлению рисками ИБ, обеспечивая уровень рисков ИБ, не превышающий установленных значений толерантности к риску. Регулярное рассмотрение рисков ИБ должно проходить на уровне руководства организации
Определение недопустимых событий (ОЗН-03)	На уровне руководства риски ИБ рассматриваются как недопустимые события. В рамках данного процесса производится выявление и уточнение недопустимых событий

Второй блок процессов, обеспечивающих корпоративную ИБ, состоит из восьми частей, содержащих группы процессов:

1. Процессы планирования и организации деятельности (ПОД);
2. Процессы по работе с персоналом (РП);
3. Процессы юридической поддержки (ЮП);
4. Процессы физической безопасности (ФБ);
5. Процессы в области непрерывности бизнеса (НБ);
6. Процессы разработки, приобретения и внедрения (РПВ);
7. Процессы обслуживания, поддержки и восстановления (ОПВ);
8. Процессы мониторинга оценки и анализа (МОА).

Описание этих групп процессов приведено ниже.

Наименование группы блока процессов, обеспечивающих корпоративную ИБ	Описание процесса
Процессы планирования и организации деятельности (ПОД)	В этой группе описываются процессы планирования и организации деятельности в области обеспечения ИБ. Сюда включается управление рисками ИБ, управление стратегией ИБ и архитектурой ИБ, управление бюджетом и затратами, построение СУИБ, управление соглашениями об уровне услуг и подрядчиками, а также управление программой bug bounty
Процессы по работе с персоналом (РП)	В данной группе описываются процессы по работе с персоналом организации в части определения обязательств, управления компетенциями, повышения осведомленности, привлечения к дисциплинарной ответственности в случае нарушения требований ИБ
Процессы юридической поддержки (ЮП)	Юридическая поддержка необходима для отслеживания изменений в законодательстве. В эту группу входят процессы юридической поддержки защиты ПДн и КТ, обеспечения юридически значимых обязательств в области ИБ контрагентов, специальная юридическая поддержка, заключающаяся в обеспечении специфичных требований законодательства к тому или иному виду деятельности, а также претензионно-исковая работа в отношении физических и юридических лиц, нарушивших требования ИБ
Процессы физической безопасности (ФБ)	В данной группе находятся процессы обеспечения физической безопасности в границах и за границей контролируемой зоны организации
Процессы в области непрерывности бизнеса (НБ)	В этой группе находятся процессы по разработке планов непрерывности бизнеса в отношении инцидентов ИБ, а также учета требований ИБ при разработке планов непрерывности бизнеса
Процессы разработки, приобретения и внедрения (РПВ)	В данной группе находятся процессы управления проектами, требованиями, изменениями, доступностью и мощностью, выбором и внедрением решений, управления активами и конфигурациями
Процессы обслуживания, поддержки и восстановления (ОПВ)	Эта группа процессов отвечает за операционную деятельность функции ИБ и включает управление эксплуатацией, проблемами, обеспечением непрерывности деятельности, управление услугами, управление контролями бизнес-процессов, управление инцидентами ИБ и расследование инцидентов ИБ
Процессы мониторинга оценки и анализа (МОА)	Данная группа процессов, предназначенная для отслеживания эффективности применяемых мер защиты и процессов, включает верификацию недопустимых событий, внутренний аудит, мониторинг и оценку соответствия внешним требованиям, мониторинг производительности СОИБ, мониторинг, оценку и анализ системы внутреннего контроля, мониторинг, оценку и анализ соответствия внешним требованиям

Ниже по группам приведено описание всех процессов из второго блока.

Процессы планирования и организации деятельности (ПОД)

Наименование процесса	Описание процесса
Управление рисками (ПОД-01)	Руководство устанавливает процесс операционного управления рисками ИБ, который направлен на выявление, оценку и снижение IT-рисков. На уровне руководства ИБ и IT осуществляется операционное управление рисками ИБ
Управление стратегией (ПОД-02)	Процесс создания и внесения изменений в стратегию ИБ организации. Стратегия ИБ задает направление развития ИБ в организации и должна быть согласована с IT-стратегией и общей стратегией организации
Управление архитектурой организации (ПОД-03)	В данном процессе требования ИБ встраиваются в IT-архитектуру предприятия и преобразуются в формальную архитектуру ИБ. Архитектура ИБ отвечает за выработку наиболее безопасных IT-решений, обеспечение исполнения требований безопасности при построении сетей, информационных систем и приложений
Управление бюджетом и затратами (ПОД-04)	Управление бюджетом важный аспект построения СОИБ. Бюджет должен позволять осуществлять запланированные мероприятия и обеспечивать функционирование и планируемое развитие СОИБ

Наименование процесса	Описание процесса
Управление безопасностью (ПОД-05)	Построение системы управления информационной безопасностью. Например, в соответствии со стандартом ISO 27001
Управление соглашениями об услугах (ПОД-06)	Услуги ИБ должны иметь согласованные с заинтересованными сторонами параметры их предоставления. Например, если SOC работает только 8 часов 5 дней в неделю, то это может серьезно повлиять на его возможности реагирования на инциденты ИБ
Управление подрядчиками (ПОД-07)	Модель потребления IT-услуг может быть разной, часть услуг может быть выведена на аутсорсинг; например, можно закупить услуги SOC. В случае вывода услуг ИБ на аутсорсинг необходимо управлять SLA предоставляемых услуг. Для этого необходимо измерять параметры данных услуг и взаимодействовать с их поставщиками
Управление программой bug bounty (ПОД-08)	Управление программой bug bounty является отдельным процессом, так как требует постоянного мониторинга результатов и отслеживания ее эффективности. Например, назначенное вознаграждение может оказаться слишком низким, и желающих участвовать в такой программе не будет. Все выявленные результаты необходимо оценивать для осуществления выплат за найденные уязвимости. Выявленные уязвимости будут являться входами для совершенствования как самих средств защиты, так и процессов обеспечения ИБ

Процессы по работе с персоналом (HR)

Наименование процесса	Описание процесса
Обеспечение требований ИБ при рекрутинге и увольнении (РП-01)	При поиске кандидатов, устройстве на работу и оформлении трудовых отношений необходимо соблюдение формальных требований ИБ. Применение некоторых средств защиты требует оформления согласия на их использование. Без должного оформления и прекращения трудовых отношений с работником сложно привлечь его к ответственности в случае наступления инцидентов ИБ
Управление квалификацией в области ИБ (РП-02)	Квалификацией персонала следует управлять на регулярной основе. Это касается специалистов в области ИБ и IT, которым необходимы актуальные специализированные знания в области управления средствами защиты информации и внутренних процессов организации работы подразделений
Привлечения работника к дисциплинарной ответственности (РП-03)	В случае нарушения требований ИБ работники должны привлекаться к дисциплинарной ответственности в зависимости от степени тяжести проступка. Процесс привлечения к дисциплинарной или иной ответственности может являться результатом расследования инцидента информационной безопасности
Повышение осведомленности в вопросах ИБ (РП-04)	Мероприятия по повышению осведомленности включают не только обучение, но и проведение учений, имитирующих действия злоумышленника (например, рассылка «фишинговых» писем и последующая регистрация перехода работника по ссылкам, содержащимся внутри письма)

Юридическая поддержка

Наименование процесса	Описание процесса
Юридическая поддержка защиты ПДн и КТ (ЮП-01)	Законодательство в области ПДн стремительно развивается во всем мире. Принятие новых законодательных требований в области ПДн нуждается в их мониторинге и оценке влияния на организацию
Юридическая поддержка договорной деятельности (ЮП-02)	Отношения между организациями должны сопровождаться обязательствами по сохранению информации контрагента. Некоторая информация может быть передана другой организации для проведения тех или иных работ. Услуги информационной безопасности также могут закупаться у сторонней организации. Во всех вышеперечисленных вопросах необходимо юридически значимо закрепить ответственность
Специальная юридическая поддержка (ЮП-03)	Специальные виды тайн, а также специальные законы, регулирующие те или иные виды деятельности, также нуждаются в их проработке

Разработка, приобретение и внедрение

Наименование процесса	Описание процесса
Управление программами и проектами (РПВ-01)	Законодательство в области ПДн стремительно развивается во всем мире. Принятие новых законодательных требований в области ПДн нуждается в их мониторинге и оценке влияния на организацию
Управление выявлением требований (РПВ-02)	Процесс обеспечивает учет требований ИБ в бизнес-процессах, приложениях, обработке информации, инфраструктуре и услугах
Управление изменениями (РПВ-03)	Процесс обеспечивает контроль изменений в IT-инфраструктуре, в том числе внесение изменений в средства защиты информации в соответствии с процессом управления изменениями. Рекомендации по контролю изменений размещены по ссылке
Управление передачей и приемкой изменений (РПВ-04)	Приемка и ввод в эксплуатацию новых решений, конвертация данных, приемочные испытания, ввод в эксплуатацию новых или измененных бизнес-процессов и IT-услуг должны проходить под контролем службы ИБ и с учетом требований ИБ
Управление доступностью и мощностью (РПВ-05)	Данный процесс отвечает за планирование доступности и мощности средств защиты информации, используемых в организации
Управление выбором и внедрением решений (РПВ-06)	Процесс обеспечивает учет требований ИБ при выборе и внедрении решений IT и ИБ в организации
Управление IT-активами (РПВ-07)	Процесс обеспечивает обнаружение, отслеживание и управление программными и аппаратными IT-активами на протяжении всего их жизненного цикла. Как процесс управления IT-активами связан с кибербезопасностью, описано в статье
Управление конфигурациями (РПВ-08)	Процесс управляет информацией о связях между IT-активами и требованиями ИБ по настройке IT-активов. Используется функцией ИБ для понимания связей межу IT-активами и для предъявления требований к конфигурации IT-активов

Физическая безопасность

Наименование процесса	Описание процесса
Безопасность в контролируемой зоне (ФБ-01)	Должна быть обеспечена физическая безопасность в контролируемой зоне. В зависимости от конфиденциальности обрабатываемой информации должны применяться те или иные методы обеспечения ИБ. Серверные и кроссовые помещения должны быть защищены от несанкционированного доступа
Безопасность в неконтролируемой зоне (ФБ-02)	Обеспечение безопасности информации и оборудования в неконтролируемой зоне осуществляется обычно за счет шифрования информации и ответственных действий работников с выносимым оборудованием

Непрерывность бизнеса

Наименование процесса	Описание процесса
Разработка планов непрерывности на случай инцидентов ИБ (НБ-01)	Некоторые инциденты ИБ могут серьезно повлиять на деятельность организации. Данный процесс обеспечивает формирование планов непрерывности деятельности организации на случай наступления инцидентов ИБ. Стоит помнить, что иногда восстановление невозможно без актуальных резервных копий
Учет требований ИБ при разработке планов непрерывности (НБ-02)	Данный процесс обеспечивает исполнение требований ИБ при разработке планов непрерывности. Общее требование заключается в том, что уровень ИБ не должен быть ниже установленного в организации в течение долгого периода времени

Обслуживание, поддержка и восстановление

Наименование процесса	Описание процесса
Управление эксплуатацией (ОПВ-01)	Процесс отвечает за эксплуатацию средств защиты информации. Как и любое другое оборудование, средства защиты информации нуждаются в техническом обслуживании и устранении инцидентов, связанных с их отказами или некорректной работой
Управление проблемами (ОПВ-02)	Отказы технических средств защиты информации могут повторяться неоднократно; также могут возникать другие проблемы, связанные с их работой (конфликты между собой, невозможность работы с используемым оборудованием и ПО). Такие проблемы необходимо решать в рамках формализованного процесса
Управление доступом (ОПВ-03)	Данный процесс отвечает за управление доступом в организации. Управление доступом является важной составляющей обеспечения ИБ организации. Доступ работников должен быть сведен к необходимому для исполнения своих должностных обязанностей и пересматриваться на регулярной основе. Для этого в организации необходимо разработать механизм назначения и пересмотра доступа к информационным ресурсам, оборудованию, панелям управления облачной инфраструктуры и пр.
Управление непрерывностью деятельности (ОПВ-04)	Данный процесс направлен на создание планов непрерывности деятельности (DRP disaster recovery plan) и планов восстановления. Восстановление и откат к прежнему состоянию может понадобиться и в рамках обычного обновления ПО или прошивки, поэтому разработка планов восстановления всегда производится до внесения изменений, которые могут привести к выходу из строя ИС, СЗИ и пр.

Наименование процесса	Описание процесса
Управление услугами безопасности (ОПВ-05)	Обеспечение ИБ организации следует выстраивать как предоставление некоторого объема ценных для организации услуг. Важно управлять как объемом предоставляемых услуг, так и их параметрами
Управление контролями бизнес-процессов (ОПВ-06)	В бизнес-процессах должны быть предусмотрены контрольные процедуры для обеспечения ИБ
Управление инцидентами ИБ (ОПВ-07)	Обнаружение инцидентов ИБ может быть осуществлено с помощью технических средств или вручную по сигналу от собственного персонала, работников контрагента или по требованию государственного органа
Расследование инцидентов (ИБ ОПВ-08)	Некоторые инциденты ИБ нуждаются в расследовании, а соответственно и привлечении компетентных специалистов и, возможно, компетентных органов для проведения расследования и привлечения к ответственности виновных лиц

Мониторинг, оценка и анализ

Наименование процесса	Описание процесса
Мониторинг, оценка и анализ производительности и соответствия СОИБ (МОА-01)	Данный процесс обеспечивает сбор, проверку и оценку целей и метрик производительности и соответствия СОИБ
Мониторинг, оценка и анализ системы внутреннего контроля (МОА-02)	Процесс обеспечивает мониторинг, оценку и анализ механизмов внутреннего контроля, относящихся к информационной безопасности
Мониторинг, оценка и анализ соответствия внешним требованиям (МОА-03)	Данный процесс обеспечивает проведение мониторинга, оценки и анализа внешних требований по отношению к организации. Такими требованиями могут выступать как требования закона, так и договорные обязательства в области ИБ
Верификация недопустимых событий (МОА-04)	Данный процесс обеспечивает верификацию недопустимых событий. Подробнее о верификации недопустимых событий можно прочитать в статье Порядок проведения верификации недопустимых событий
Внутренний аудит ИБ (МОА-05)	Данный процесс обеспечивает проведение внутреннего аудита ИБ

5. Заключение

Сформированная процессная модель дает общее представление об основных процессах, участвующих в обеспечении ИБ организации, показывает развитие процессов ИБ, а также связь этих процессов между собой. Воспользовавшись моделью, можно получить представление о работе функции ИБ в организации, выстроить взаимодействие с другими функциями (подразделениями) организации. В модели подчеркнута роль руководства организации в оценке, задании направления развития и мониторинге информационной безопасности. Модель может быть доработана под нужды конкретной организации путем добавления дополнительных процессов. Отсутствие же обозначенных в нашем фреймворке процессов может негативно сказаться на эффективности ИБ в организации.