Лекция_4. Управление информационной безопасностью

Управление информационной безопасностью (Information Security Management или ISM) - процесс, который обеспечивает*конфиденциальность*, *целостность* и доступность активов, информации, данных и услуг организации. *Управление информационной безопасностью* обычно является частью Организационного подхода к Управлению безопасностью, который имеет более широкую область охвата, чем поставщик услуг, и включает обработку бумажных документов, *доступ* в здания, телефонные звонки и т.п., для всей организации[1].

Основной целью *ISM* является обеспечение эффективного управления информационной безопасностью всех услуг и деятельностей в рамках Управления услуг. *Информационная безопасность* предназначена для защиты от нарушения конфиденциальности, доступности и целостности информации, информационных систем и коммуникаций.

1. **Конфиденциальность** - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
2. **Целостность** - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
3. **Доступность** - состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно[15].

Цель обеспечения информационной безопасности достигнута, если:

1. Информация доступна тогда, когда это требуется, а информационные системы устойчивы к атакам, могут избегать их или быстро восстанавливаться.
2. Информация доступна только тем, кто имеет соответствующие права.
3. Информация корректна, полна и защищена от неавторизованных изменений.
4. Обмен информацией с партнерами и другими организациями надежно защищен.

Бизнес определяет, что и как должно быть защищено. При этом для эффективности и целостности обеспечения информационной безопасности необходимо рассматривать бизнес процессы от начала до конца, так как слабое *место* может сделать уязвимой всю систему.

Процесс *ISM* должен включать в себя:

- формирование, управление, распространение и соблюдение Политики информационной безопасности и других вспомогательных политик, которые

имеют отношение к информационной безопасности. **Политика информационной безопасности (Security Policy)** - политика, определяющая подход организации к управлению информационной безопасностью [1].

- понимание согласованных текущих и будущих требований бизнеса к безопасности;
- использование *контролей безопасности* для выполнения Политики информационной безопасности и управления рисками, связанными с доступом к информации, системам и услугам. Термин "*контроль безопасности*" является заимствованным из английского языка и в данном контексте означает набор контрмер и мер предосторожности, применяемых для аннулирования, уменьшения рисков и противостояния им. То есть *контроль безопасности* состоит из проактивных и реактивных действий;
- документирование перечня *контролей безопасности*, действий по их эксплуатации и управлению, а также всех связанных с ними рисков;
- управление поставщиками и контрактами, требующими доступа к системам и услугам. Осуществляется при взаимодействии с процессом Управления поставщиками;
- контроль всех "брешей" безопасности и инцидентов, связанных с системами и услугами;
- проактивное улучшение *контролей безопасности* и уменьшение рисков нарушения информационной безопасности;
- интеграция аспектов информационной безопасности во все процессы Управления услуг.

Политика информационной безопасности должна включать в себя следующее:

- реализация аспектов Политики информационной безопасности;
- возможные злоупотребления аспектами Политики информационной безопасности;
- политика контроля доступа;
- *политика использования* паролей;
- политика электронной почты;
- политика интернета;
- политика антивирусной защиты;
- политика классификации информации;
- политика классификации документов;
- политика удаленного доступа;
- политика доступа поставщиков к услугам, информации и компонентам;
- политика размещения активов.

Перечисленные политики должны быть доступны пользователям и заказчикам, которые в свою *очередь* обязаны письменно подтвердить свое согласие с ними.

Политики утверждаются руководством бизнеса и IT и пересматриваются в зависимости от обстоятельств.

Чтобы обеспечивать информационную *безопасность* и управлять ею, необходимо поддерживать Систему управления информационной безопасностью. **Система управления информационной безопасностью (Information Security Management System или ISMS)** - система политик, процессов, стандартов, руководящих документов и средств, которые обеспечивают организации достижение целей управления информационной безопасностью[1]. На рис. 4.3 показана структура ISMS, наиболее широко используемая организациями.

Рис. 4.3. ISMS

На рис. 4.3 представлены 5 элементов структуры ISMS:

1. Контроль. Цели контроля:
   - формирование системы управления информационной безопасностью в рамках организации;
   - формирование организационной структуры для подготовки, утверждения и реализации Политики информационной безопасности;
   - распределение ответственностей;

- формирование документации по контролю.

2. Планирование. Цель планирования - разработать и рекомендовать подходящие метрики и способы измерения информационной безопасности. В первую очередь планирование должно учитывать требования и особенности конкретной организации. Источниками информации для формирования требований к информационной безопасности являются бизнес, риски, планы, стратегия, соглашения (в первую очередь OLA и SLA). При этом важно учитывать моральную, законодательную и этическую ответственности в контексте информационной безопасности.
3. Реализация. Цель реализации - обеспечение подходящих процедур, инструментов и *контролей безопасности* для поддержки Политики информационной безопасности.

   В рамках реализации проводятся следующие мероприятия:

   - *идентификация активов* - совместно с Управлением конфигурациями;
   - классификация информации - информация и информационные хранилища должны быть классифицированы в соответствии с их чувствительностью и значимостью по отношению к трем аспектам информационной безопасности (конфиденциальности, целостности, доступности).
4. Оценка. Цель оценки в рамках ISMS:
   - проверка соответствия политики информационной безопасности требованиям к информационной безопасности из SLA и OLA;
   - проведение регулярных проверок технической составляющей информационной безопасности для IT систем;
   - предоставление информации для регуляторов и внешних аудиторов при необходимости;
5. Поддержка. Цели поддержки ISMS:
   - улучшение соглашений в отношении информационной безопасности, например, SLA и OLA
   - совершенствование средств и контролей информационной безопасности[10].

Ключевые деятельности в рамках *ISM*:

1. формирование, пересмотр и корректирование Политики информационной безопасности и набора поддерживающих ее вспомогательных политик;
2. реализация и соблюдение политик информационной безопасности, а также обеспечение взаимодействия между ними;
3. оценка и классификация всех информационных активов и документов;

4. использование, пересмотр и корректирование набора *контролей безопасности*, мер по оценке рисков и ответных действий;
5. мониторинг и управление "брешами" безопасности и инцидентами;
6. анализ, ведение отчетности и уменьшение влияния "брешей" в безопасности и инцидентов;
7. составление расписания и проведение аудитов, тестирования и обзоров.

Взаимодействие указанных деятельностей представлено на рис. 4.4.

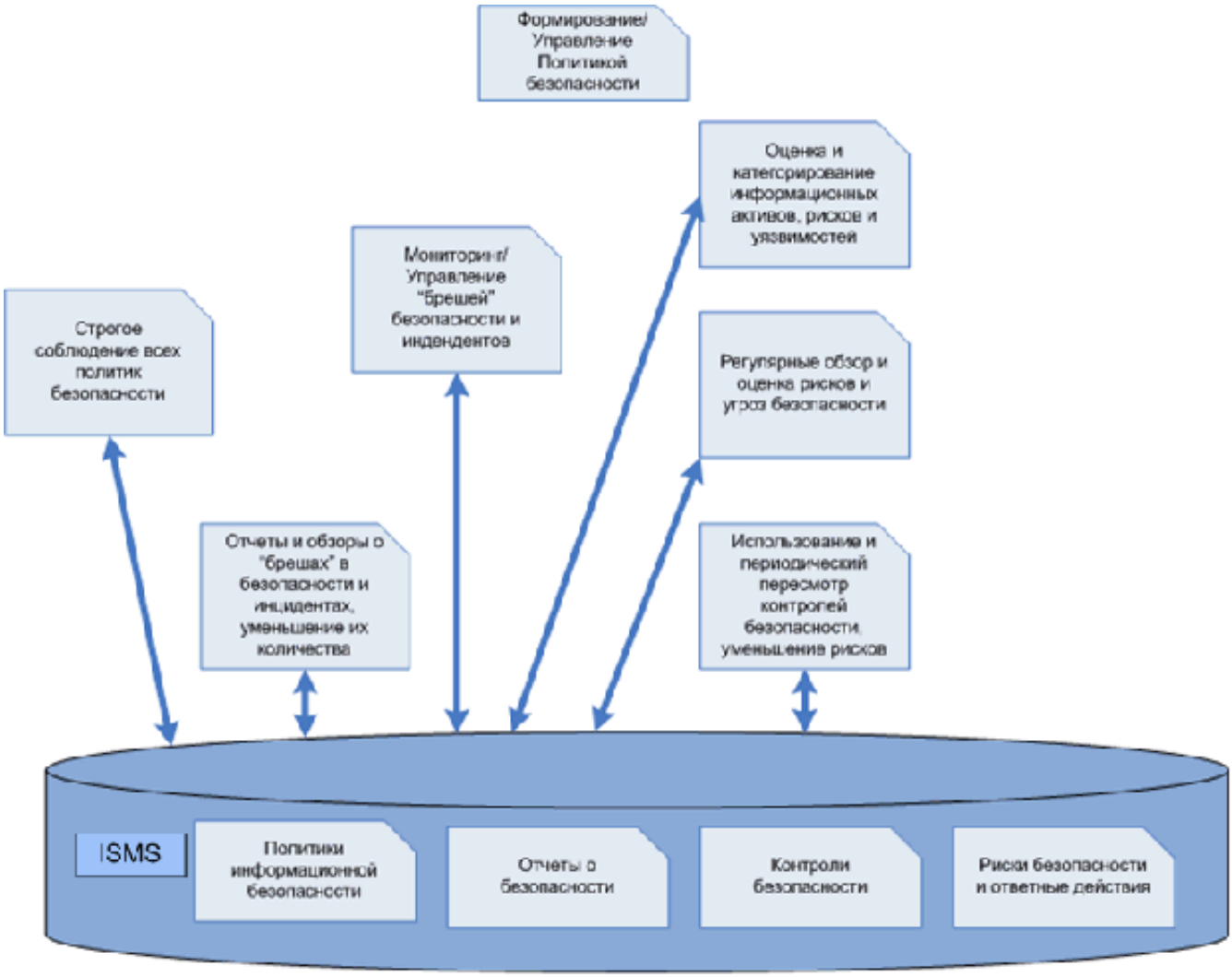

Рис. 4.4. Ключевые деятельности в рамках ISM

Для обеспечения и поддержки Политики информационной безопасности необходимо сформировать и использовать набор *контролей безопасности*. Для предотвращения инцидентов и правильного реагирования в случае их возникновения используют меры безопасности, представленные на рис. 4.5.

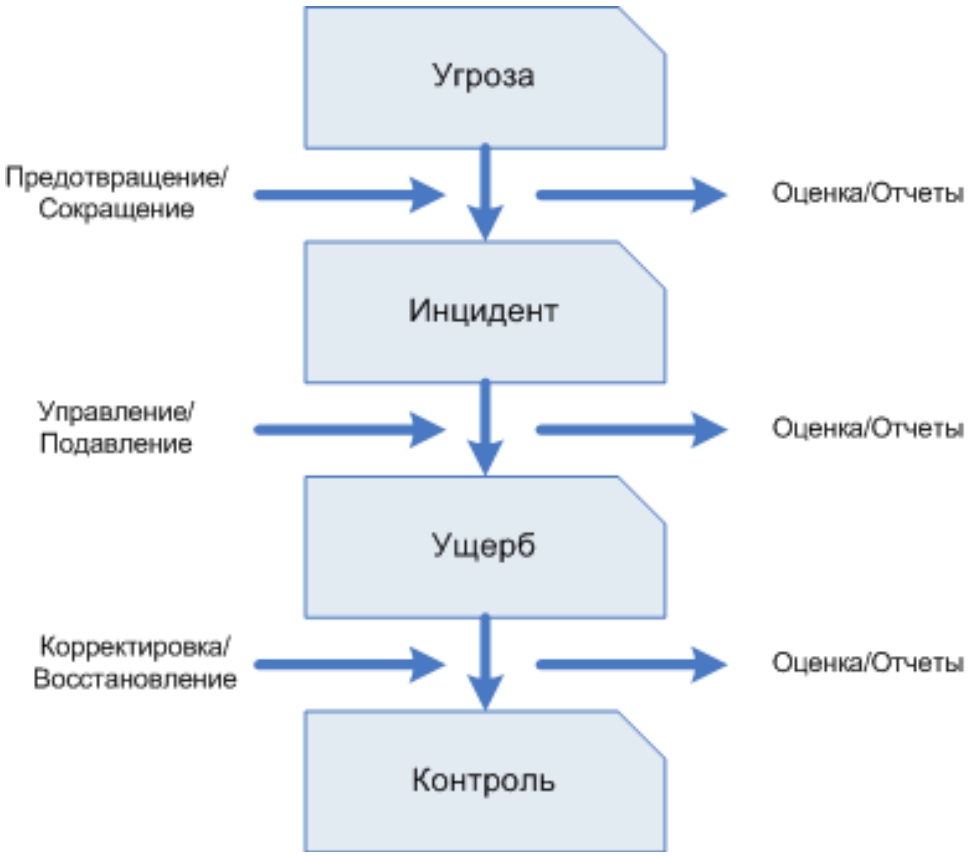

Рис. 4.5. Контроли безопасности

На рис. 4.5 выделено четыре стадии. Первая стадия - возникновение угрозы. Угрозой является все, что может негативно повлиять на *бизнес-процесс* или прерывать его. Инцидент - это реализованная *угроза*. Инцидент является отправной точкой для применения *контролей безопасности*. В результате инцидента появляется *ущерб*. Для управления или устранения рисков также применяются контроли безопасности. Для каждой стадии необходимо подобрать подходящие меры обеспечения информационной безопасности:

1. превентивные - меры безопасности, которые предотвращают появление инцидента информационной безопасности. Например, распределение прав доступа.
2. восстановительные - меры безопасности, направленные на уменьшение потенциального ущерба в случае инцидента. Например, резервное копирование.
3. обнаруживающие - меры безопасности, направленные на обнаружение инцидентов. Например, антивирусная защита или система обнаружения вторжений.
4. подавляющие - меры безопасности, которые противодействуют попыткам реализации угрозы, то есть инцидентам. Например, банкомат забирает у клиента карту после определенного количества неправильных вводов PIN-кода.

5. корректирующие - меры безопасности, направленные на восстановления после инцидента. Например, восстановление резервных копий, откат на предыдущее рабочее состояние и т.п.

Входами процесса *ISM* являются:

1. информация от бизнеса - стратегии, планы, бюджет бизнеса, а также его текущие и будущие требования;
2. политики безопасности бизнеса, планы безопасности, Анализ рисков;
3. информация от IT - стратегия, планы и бюджет IT;
4. информация об услугах - информация от *SLM*, в частности Портфеля услуг и Каталога услуг, SLA/*SLR*;
5. отчеты процессов и анализа рисков от *ISM*, Управления доступностью и Управления непрерывностью услуг;
6. детальная информация обо всех инцидентах информационной безопасности и "брешах" в ней;
7. информация об изменениях - информация от процесса Управления изменениями, в частности расписание изменений и их влияние на планы, политики и контроли информационной безопасности;
8. информация о взаимоотношениях бизнеса с услугами, вспомогательными услугами и технологиями;
9. информация о доступе партнеров и поставщиков к услугам и системам, предоставляемая процессами Управления поставщиками и Управления доступностью.

Выходами *ISM* являются:

1. всеобъемлющая Политика информационной безопасности и другие вспомогательные политики, которые имеют отношение к информационной безопасности;.
2. Система управления информационной безопасностью (ISMS), которая содержит всю информацию, необходимую для обеспечения *ISM*;
3. результаты переоценки рисков и ревизии отчетов;
4. набор *контролей безопасности*, описание их эксплуатации и управления, а также всех связанных с ними рисков;
5. аудиты информационной безопасности и отчеты;
6. расписание тестирования планов информационной безопасности;
7. классификация информационных активов;
8. отчеты о существующих "брешах" в информационной безопасности и инцидентах;
9. политики, процессы и процедуры для управления доступом поставщиков и партнеров к услугам и системам.

В качестве ключевых показателей производительности процесса Управления информационной безопасностью можно использовать множество метрик, например:

1. защищенность бизнеса от нарушений информационной безопасности
   - процентное уменьшение сообщений о "брешах" в Сервис-деск;
   - процентное уменьшение негативного влияния на бизнес со стороны "брешей" и инцидентов;
   - процентное увеличение пунктов, касающихся информационной безопасности, в SLA.
2. формирование четкой и согласованной политики информационной безопасности, учитывающей потребности бизнеса, то есть уменьшение количества несовпадений между процессами *ISM* и процессами и политиками информационной безопасности бизнеса.
3. процедуры по обеспечению безопасности, которые оправданы, согласованы и утверждены руководством организации:
   - увеличение согласованности и пригодности процедур обеспечения безопасности;
   - увеличение поддержки со стороны руководства
4. механизмы улучшения:
   - количество предложенных улучшений в отношении контролей и процедур;
   - уменьшение количества несовпадений, обнаруженных в процессе тестирования и аудита.
5. информационная безопасность является неотъемлемой частью услуг и процессов *ITSM*, то есть увеличение количества услуг и процессов, в которых предусмотрены меры безопасности[10].

ISM сталкивается со множеством трудностей и рисков на пути обеспечения информационной безопасности. К сожалению, на практике достаточно часто бизнес считает, что вопросами информационной безопасности должна заниматься только IT. Еще хуже, когда бизнес не понимает, зачем вообще нужно уделять внимание информационной безопасности. Создание эффективной системы защиты информации влечет за собой большие *затраты*, которые должны быть понятны руководству, так как именно оно принимает решение о финансировании. При этом важно соблюдать баланс - обеспечение информационной безопасности не должно стоить больше самой защищаемой информации