KPMG

KPMG – построение стратегии кибербезопасности

14 июня

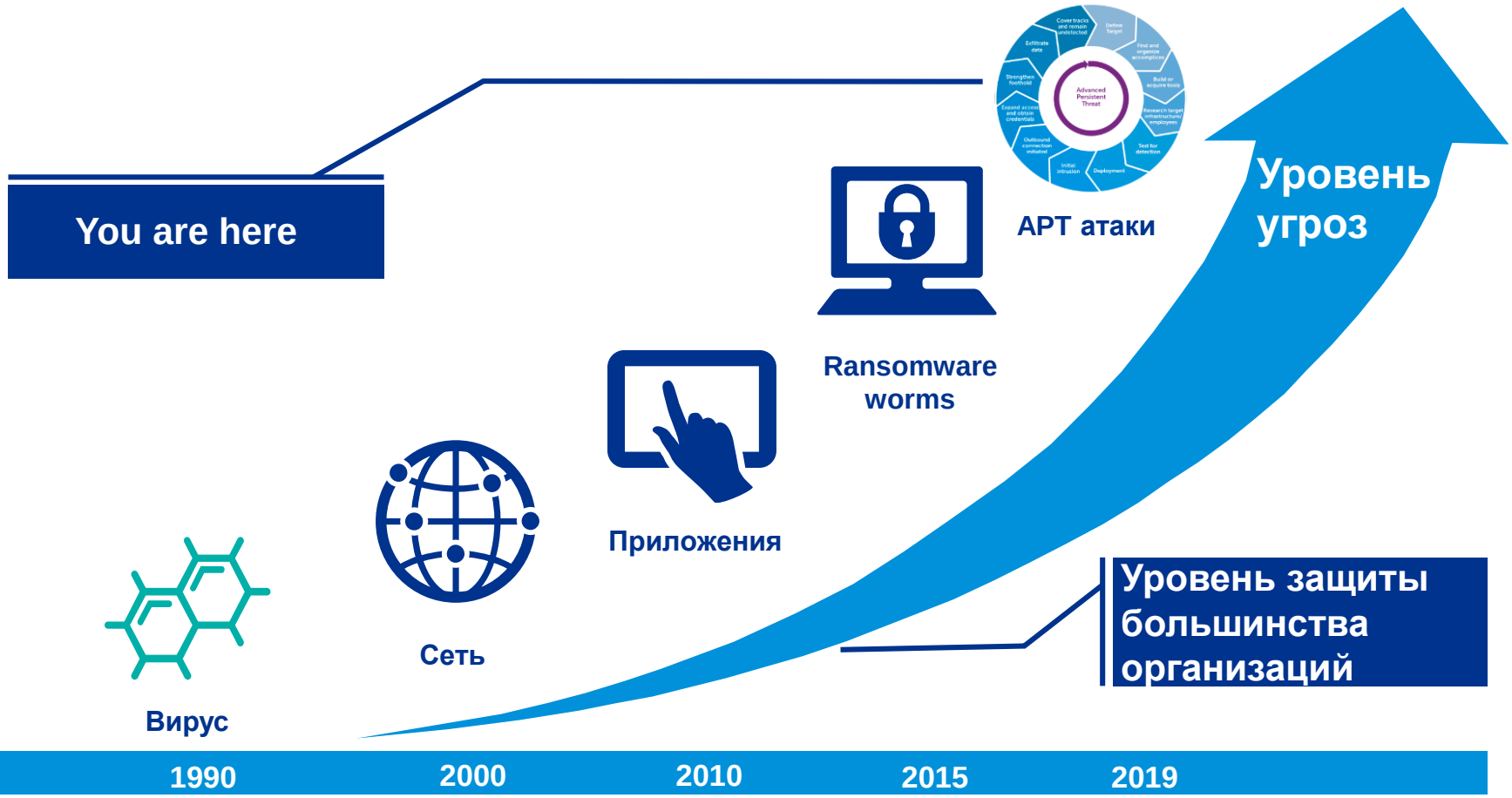
Елена Герасименко

Старший консультант

KPMG

Современный ландшафт ИТ безопасности

Развитие вектора атак



Недавние инциденты безопасности

Январь 2019

Исследователи зафиксировали масштабную вредоносную кампанию, жертвами которой уже стали более 1 млн пользователей Mac. В ходе операции, начавшейся 11 января текущего года, злоумышленники распространяют вредоносное ПО Shlayer через рекламное изображение.

Код встраивается непосредственно в изображение с помощью стеганографии – популярного метода, используемого для распространения вредоносных программ.

Апрель 2019

Министерство иностранных дел Бельгии было вынуждено на целый день отключить свои электронные сервисы, в том числе выдачу паспортов и легализацию документов из-за кибератаки.

Сеть Diplobel, связывающая министерство с посольствами и консульствами по всему миру, была полностью отключена. На восстановление ее работы потребовалось около 72 часов.

Март 2019

Злоумышленники распространяли вредоносное ПО, получая доступ к банковским реквизитам. Затем преступники перечисляли деньги на другие счета.

При этом вредоносная программа блокировала уведомления о списании денежных средств и жертвы не получали соответствующие уведомления.

Май 2019

Обнаружен новый бэкдор, специально созданный для атак на серверы Microsoft Exchange. Вредоносная программа под названием LightNeuron работает как агент пересылки сообщений, позволяя операторам контролировать все данные, проходящие через инфицированный почтовый сервер.

Злоумышленники могут не только перехватывать, но также отправлять, переадресовывать, блокировать и редактировать письма.

APT – атаки. Этапы развития атаки

Атака посредника. Man-in-the-middle attack

Атака посредника — вид атаки в криптографии, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом. Является методом компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.

Способом защиты от от этой атаки перехвата информации является шифрование.

Если одно из этих правил не соблюдено - весь протокол скомпрометирован

Обеспечение безопасности протокола связи

Атака на водопое. Watering hole attack

Стратегия атаки, в которой жертва - конкретная группа. Нападавший предполагает или наблюдает, какие веб-сайты группа часто использует и заражает один или несколько из них вредоносными программами.

- Обеспечение обновления ПО и операционных систем до последних версий
- Проверка правильной настройки конфигурации брандмауэров и других продуктов безопасности
- Немедленная блокировка трафика на все ресурсы, о компрометации которых становится известно, уведомление владельцев ресурсов.
- Инспекция всех популярных веб-сайтов, которые сотрудники посещают и проверка этих ресурсов на постоянной основе на предмет вредоносного программного обеспечения
- Обучение сотрудников, особенно с доступом к критическим данным и инфраструктуре
- Настройка браузеров или других инструментов для уведомления пользователей об
- Регулярная проверка внутренних и внешних ресурсов, принадлежащих компании, с целью удостовериться, что они безопасны

Атака цепочки поставок. Supply chain attack

Метод состоит из внедрения вредоносного кода в заведомо полезное или доверенное ПО.

Например:

Злоумышленники скомпрометировали сервер поддержки одного из поставщиков программного обеспечения и рассылали его клиентам набор вредоносов под видом обновлений. Как сообщают исследователи, чтобы избежать обнаружения антивирусами, киберпреступники использовали украденный сертификат соответствия.

Исследование сетевого трафика

Хотя нападавшие могут включить различные эксплойты или инструменты в атаку, трафик генерируемый конечным вредоносным ПО во время связи с серверами командования и управления остается специфическим. Обнаруживая эту коммуникацию, организации могут запустить приготовленные меры безопасности, чтобы предотвратить дальнейшее развитие нападения. Необходимо не только отслеживать подозрительную активность в вашей сети (будь то шпионаж или другие виды киберпреступлений), но и расследовать инциденты и выяснять, почему они произошли.

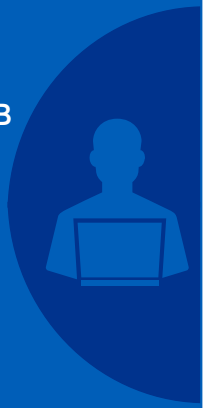
KPMG

Безопасность инфраструктуры компании

Распространенные мифы кибербезопасности …

Мифы

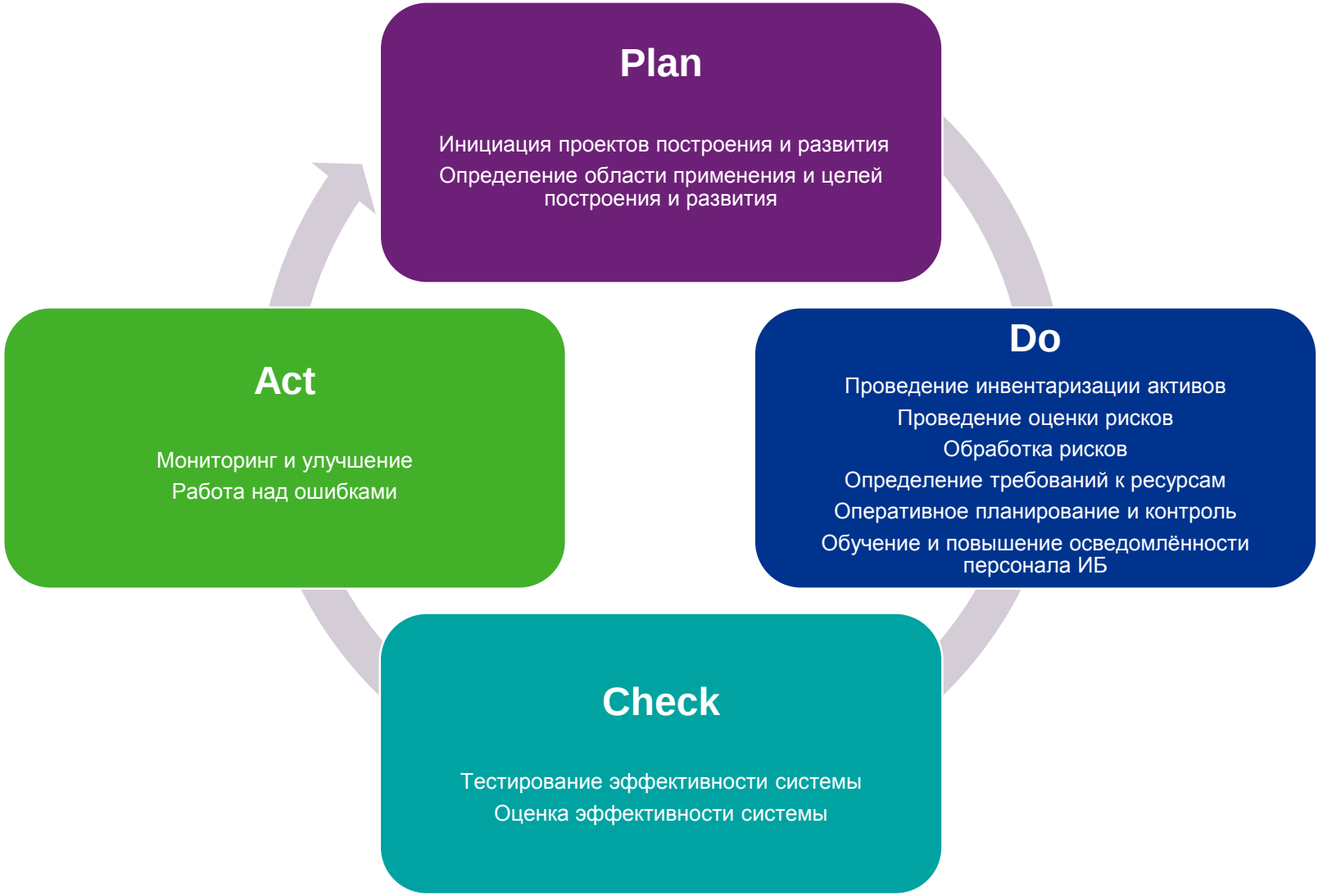
1. Мы не провайдер или ИТ-организация, и мы не зависим от общемировой ситуации, поэтому риск кибератаки низкий.
2. Кибербезопасность – это в основном о технологиях.
3. Большинство больших компаний держит кибербезопасность под контролем.
4. Кибербезопасность – это гонка вооружений между хорошими и плохими ребятами.



Факты

- Кибер-угрозы влияют на все компании, которые в работе полагаются на людей или технологии.
- Это быстро меняющийся ландшафт ожиданий рынка и клиентов.
- Большие компании обычно недостаточно подготовлены к реальной киберугрозе из-за большого размера и сложности системы.
- Киберебезопасность – это комплексный, гибкий процесс, а не отдельное решение.

Безопасность - это процесс



Области безопасности компании

Экономическая безопасность

Вопросы финансово-экономической состоятельности Компании, устойчивости к банкротству, параметры платежеспособности и другие “денежные” характеристики

Физическая безопасность

Режим, физическая охрана объектов и личная охрана руководства, противодействие физическим угрозам со стороны криминальных структур, взаимодействие с правоохранительными государственными органами

Информационная безопасность

Защита собственной информации, в том числе конфиденциальной, коммерческая разведка, информационно-аналитическая работа с внешними и внутренними субъектами и т.д.

Внутренняя безопасность

Обеспечение безопасности сотрудников Компании, проведение расследований, организация работы с коммерческой тайной, кадровая безопасность

Потенциальные проблемы безопасности

Риски, связанные с кибербезопасностью, могут иметь финансовые последствия для всех вовлеченных сторон. На основе нашего опыта в реализации проектов по услугам кибербезопасности, выделены потенциальные угрозы для бизнеса.

1	**Нормативные штрафы и компенсационные выплаты**	Ужесточение регуляторных требований и штрафов указывают на недостаточное стремление в организациях повышать зрелость управления рисками в организациях
2	**Незрелая программа кибербезопасности**	Технологический взгляд на безопасность или отсутствие взаимосвязи между общим управлением рисками и риском кибербезопасности определяет низкую зрелость программ риска
3	**Отсутствие надлежащего управления и ответственности**	Отсутствие ясности и определенности в отношении управления и владения программами риска создают риски несоблюдения нормативных обязательств (FFIEC, GLBA, PCI, CFPB и т. Д.)
4	**Ненадлежащее управление рисками третьих лиц**	Ошибка или небрежность одного лишь человека или третьей стороны могут быстро привести к значительному финансовому и репутационному ущербу
5	**Отсутствие программ защиты данных и конфиденциальности**	Отсутствие эффективной защиты данных создает риск утечки конфиденциальных данных, особенно, когда ускоренными темпами внедряются новые технологии, влекущие изменения бизнес-моделей и правил

KPMG

Стратегия

Управление кибербезопасностью - Оценка зрелости кибербезопасности

Трехэтапный подход, который предлагает KPMG представляет собой логическую последовательность действий, и гарантирует проверку результатов на каждом этапе. Помимо сверки данных, это также обеспечивает участие заинтересованных сторон в процессе модернизации инфраструктуры.

Фазы

Фаза I - сбор информации

Взаимодействовать с бизнес-лидерами, развитие понимания риска, выяснение необходимых функций безопасности

- Идентификация наиболее ценных активов
- Совместное описание рисков, возможностей, нормативных драйверов и реестра активов
- Подход к оценке зрелости
- Оценка текущего состояния
- Проверка

Фаза II - Анализ

Оценка текущих бизнес возможностей, в применении ко встроенному регистру рисков, с целью понять текущее состояние системы

- Выполнение gap анализа (люди, процессы и технологии)
- Оценка интеллектуальных угроз и ранжирование рисков на основе профиля и ландшафта
- Сравнение
- Определение неотъемлемого и конечного риска

Этап III - Стратегия и дорожная карта

Разработка потенциальных вариантов управления рисками в пределах толерантности и рекомендации по реализации дорожной карты от текущего состояния до целевого

- Разработка предложений по целевому состоянию
- Разработка рекомендаций по людям, процессам и технологиям
- Выработка инсайтов по потенциальной стратегии и дорожной карте
- Определение инициатив по улучшению

Результаты

Текущее состояние зрелости включает:

- Высоко уровневый обзор ключевых активов и рисков
- Сопоставление угроз и рисков с наиболее ценными активами
- Проверка текущего состояния технического контроля

- Ландшафт Угроз
- Неотъемлемые и конечные риски
- Регистр с классифицированными рисками и приоритетом

- Целевое состояние с дорожной картой, в которой излагаются мероприятия, которые будут проводиться в течение 2-3-х лет
- Улучшение стратегии
- Исполняемые уставы проектов для улучшения областей
- Презентация для совета директоров

Управление кибербезопасностью– Целевая операционная модель

KPMG разработала подход, где целевая операционная модель согласована с управлением кибер-рисками, стратегическими мерами с целью выявления пробелов и повышения эффективности работы, оптимизации затрат и «разумного использования» при эффективном смягчении рисков, связанных с технологией и информационной безопасностью.

Оценка текущего состояния

Оценка текущего состояния с целью определить организационное соответствие индустриальным фреймворкам для определения несоответствий и возможностей для улучшения.

Определение организационных областей, ответственных за кибербезопасность и управления рисками с целью выявления пробелов и дублирования.

Для каждой кибер и риск менеджмент деятельности определите роли, ответственности и владельцев процессов для рационализации пробелов и избыточности

Проектирование целевого состояния

Разработка целевого состояния на основе риск менеджмента и фреймворка кибербезопасности. Новое состояние должно базироваться на основе профиля кибербезопасности организации для обеспечения капиталовложения в наиболее необходимых целях.

Так как финансовые институты сталкиваются с повышенным давлением регулятора в области кибербезопасности и управления рисками, новая целевая модель должна быть разработана в соответствии с мандатами соблюдения и достижения желаемого состояния зрелости

Анализ пробелов в навыках

Проведите анализ разрыва навыков для каждой группы на основе назначенных действий в области кибербезопасности и риска, чтобы помочь обеспечить наличие соответствующих ресурсов для удовлетворения требований.

Определите критические навыки для каждой группы и разработайте стратегию удержания и обучения.

Определите и оцените возможности аутсорсинга, с целью оптимизировать затраты, а также удостоверьтесь что аутсорсинг не создает новые риски для организации.

Реализация

Определите требования для реализации целевой модели, с учетом рисков, возможностей, нормативных требований и организационной устойчивости рисков.

Обеспечьте соответствия усилий и инициатив компании с целевой моделью

Разработка коммуникационной стратегии и плана для реализации новой модели.

Переход к новой целевой модели

Непрерывная оптимизация

Обеспечьте постоянный пересмотр целевой модели с целью обеспечить:

Бизнес ориентированность на основе текущего профиля организации.

Покрытие Комплаенс требований вызванных изменениями в законодательстве

Снижение рисков кибербезопасности за счет постоянного понимания развивающейся бизнес-стратегии организации и присущего ей риска атаки или компрометации.

Управление кибербезопасностью– Целевая операционная модель

Ведущая практика в построении операционной модели управления кибербезопасностью основана на бизнес потребностях, на четко установленных принципов Управления, правах и обязанностях.

Мы поддерживаем наших клиентов в разработке стратегий для достижения целевых задач компаний. Кибербезопасность является одной из пяти главных приоритетов для исполнительного совета компании.

Бизнес ориентированный подход

Все аспекты стратегии и дорожной карты имеют четкую связь с бизнес-рисками, возможностями и нормативными драйверами;

Отслеживаемый и объективный

Методы описания текущего статуса позволяют объективно оценить статус прогресса в ходе исполнения плана работ

Выполнимый

Стратегия должна эффективно внедряться в «дорожную карту», а «дорожная карта» - в портфель с набором руководств. Нет необходимости начинать каждый этап с нуля.

Информированное управление рисками

Отслеживая и сопоставляя каждое действие к определенному риску, организация может принимать обоснованные решения по управлению рисками.

Дисциплина

Невозможно достичь зрелого состояние до тех пор пока все компоненты будут на своих местах включая право собственности, подотчетность, политику, людей, процессы, технологии и комплаенс

Комплексная модель

Фреймворк покрывает все аспекты подхода не оставляя без внимания не одну область и обеспечивая последовательность, адаптированную к уникальным характеристикам каждой организации.

Методы и инструменты для управления информационными рисками

KPMG Cyber Security Framework включает в себя как организационные компоненты, так и итеративный процесс, необходимый для обеспечения и поддержки клиентов, акционеров и сотрудников, в управлении кибер угрозами. KPMG's Cyber Security Services объединяет специалистов по защите информации и непрерывности бизнеса, управлению рисками, конфиденциальности данных, организационному дизайну, поведенческим изменениям и управлению знаниями.

Предотвратить

Услуги по приведению в соответствие элементов и аспектов кибербезопасности с динамично изменяющемся бизнес-задачами

Стратегия и управления

Улучшить

Услуги по созданию и совершенствованию программ и процессов по кибербезопасности с помощью изменений в орг. структуре и внедрения технологий

Трансформация

Обнаружить

Услуги по поддержке программ кибербезопасности, обеспечивая большую наглядность и понимание меняющихся рисков

Кибер защита

Реагировать

Услуги по обеспечению эффективно реагирования на инциденты кибербезопасности и проведению детального анализа расследования

Услуги цифрового реагирования

До взлома

После взлома

Атрибуты:

- Полнота охвата (Target Operating Model)
- Информационно-ориентированный подход

Атрибуты :

- Трансформация безопасности
- Информационно-технологическая стратегия
- Долгосрочная поставка ценностей
- Бизнес-ориентированность

Атрибуты :

- Техническая оценка
- Мониторинг безопасности
- Реакция на инцидент
- Аналитика

Атрибуты :

- Сохранение цифровых доказательств и услуги по расследованию кибербезопасности
- Анализ после взлома и расследование

Критерии оценки зрелости блока безопасности

0	**Нулевой уровень**	Полное отсутствие каких-либо процессов блока безопасности в Компании.
1	**Первый уровень (базовый)**	Существуют документальные доказательства наличия процессов. Однако процессы, лежащие в основе деятельности блока безопасности, не стандартизированы и используются нерегулярно. Не выработан общий подход к обеспечению безопасности.
2	**Второй уровень (развивающийся)**	Управленческая функция блока безопасности разработана до уровня периодически осуществляемых процессов. Однако не осуществляется регулярное обучение, и в то же время ответственность за осуществление лежит на выполняющих процессы сотрудниках.
3	**Третий уровень (установленный)**	Процессы блока безопасности стандартизированы, задокументированы и доведены до сведения сотрудников посредством обучения. Однако осуществляемые процедуры неэффективны, так как их исполнение оставлено на усмотрение персонала, что может привести к возможным нарушениям нормативных документов.
4	**Четвертый уровень (продвинутый)**	Проводятся регулярный контроль и оценка соответствия управления блока безопасности. Текущие процессы постоянно улучшаются и основаны на лучших практиках. Однако автоматизированные инструменты управления блока безопасности используются только частично.
5	**Пятый уровень (лидирующий)**	Управленческие процессы блока безопасности развиты на уровне лучших практик, постоянно улучшаются и оцениваются на зрелость по отношению другим компаниям. В результате Компания может быстро адаптироваться к любым внешним изменениям.

Подход к оценке ущерба

Предлагаемые правила оценки возможного ущерба от реализации угроз безопасности информации

Несанкционированные действия с защищаемой информацией	Вид защищаемой информации											
	Информация ограниченного доступа									Иная защищаемая информация		
	Финансово-экономического характера			Административно-управленческого характера			Технологического характера			Малая критичность	Средняя критичность	Высокая критичность
	Малая критичность	Средняя критичность	Высокая критичность	Малая критичность	Средняя критичность	Высокая критичность	Малая критичность	Средняя критичность	Высокая критичность			
Нарушение конфиденциальности информации	Низкий	Средний	Критический	Минимальный	Низкий	Средний	Низкий	Средний	Критический	Низкий	Средний	Критический
Нарушение целостности информации	Низкий	Средний	Критический	Минимальный	Низкий	Средний	Низкий	Средний	Критический	Низкий	Средний	Критический
Нарушение доступности информации	Минимальный	Низкий	Средний	Минимальный	Минимальный	Низкий	Минимальный	Низкий	Средний	Минимальный	Низкий	Средний

Пример

Минимальный ущерб – приводит к незначительным потерям материальных активов, которые быстро восстанавливаются, или к незначительному влиянию на репутацию

Низкий ущерб – вызывает заметные потери материальных активов или умеренное влияние на репутацию

Средний ущерб – приводит к значительным потерям материальных активов либо к значительному урону репутации

Критический ущерб – приводит к критическим потерям материальных активов или к полной потере репутации на рынке

Рекомендации для обеспечения соответствия требованиям

ISO 27001:2013 ISMS Current State Assessment
Systematic and Control Requirements Checklist
Internal

Scoring	
2	Fully Implemented
1	Partially Implemented
0	Not Implemented

Sr. no.	Control Objective	Detailed Control	Control Check	Observation	Gap	Reference Documents
SYSTEMATIC REQUIREMENT CHECKLIST						
4	**Context of The Organization**					
4.1	Understanding the organization and its context	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its ISMS.	1) Issue register listing external and internal issues registered.	Общие Положения Политики ИБ		Политика по ИБ_2015 с изменениями
4.2	Understadning the needs and expectation of interested parties	The organization shall determine a) Interested parties relevant to ISMS b) the requirement of these parties relevant to the ISMS	1) List of interested parties relevant to ISMS 2) The list entails the requirements of each interested party to the ISMS	Общие Положения Политики ИБ		Политика по ИБ_2015 с изменениями
4.3	Determining the scope of the ISMS	The organization shall determine the boundaries and applicability of the ISMS to establish the scope	1) Organization has considered the external and internal issues when determining the scope	Общие Положения Политики ИБ		Политика по ИБ_2015 с изменениями
			2) Organization has considered the requirements of the interested parties	Общие Положения Политики ИБ		Политика по ИБ_2015 с изменениями
			3) Interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations are considered in			Политика по ИБ_2015 с изменениями

Пример

План перехода к целевой модели функции безопасности

№ п/п	Описание рекомендации	Рекомендуемый срок исполнения							
		2019				2020			
		I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
	Информационная безопасность								
1	**Руководство и обеспечение работы по направлению ИБ**								
	Внедрить технологии автоматизированного анализа данных			■	■				
	Принять международный стандарт ISO/IEC 27001 в качестве основы построения документированной системы управления информационной безопасностью в Компании.		■	■					
	Определить перечень актуальных угроз информационной безопасности в рамках бизнес-процессов Компании, используемых информационных ресурсов и применяемых в Компании мер защиты			■					
	Создать единую информационную систему безопасности, объединяющую все текущие ИТ-решения (АРМ-системы и др.), используемые ДЭБ			■	■	■			
2	**Расследование инцидента ИБ**								
	Автоматизировать Workflow/Dataflow и роботизировать процедуры проведения служебных расследований				■	■			
3	**Изменение и актуализация ВНД**								
	Разработать обязательные с точки зрения международного стандарта ISO/IEC 27001 внутренние нормативные документы, в том числе, Политику обеспечения ИБ, Политику по оценке и обработке рисков, Политику управления доступом, Процедуру управления инцидентами, Политику обеспечения непрерывности бизнеса		■	■	■				
	Актуализировать и структурировать существующие ВНД в области информационной безопасности, определить сроки и условия пересмотра документов, распространить их действие на управляемые предприятия		■	■	■				
	Создать реестр ВНД в области обеспечения ИБ.	■							

Пример

KPMG

Спасибо!