30 июня 2025

Информационная безопасность: стратегия заказчика и подход поставщика

Современный ландшафт киберугроз меняется стремительно: атаки становятся сложнее, их последствия — масштабнее, а требования регуляторов — жестче. В таких условиях классический подход к обеспечению информационной безопасности, основанный исключительно на технологических решениях, уже не работает. Сегодня эффективная защита цифровых активов требует комплексного подхода, объединяющего технологии, процессы и людей.

Как крупные корпорации и поставщики ИБ-услуг выстраивают свою защиту? В чем их стратегии схожи, а в чем принципиально различаются? Мы решили взглянуть на эти вопросы через призму двух экспертных мнений: **Александра Шепилова, директора направления обеспечения ИБ корпоративных информационных систем «Ростелекома»**, и **ведущего архитектора по информационной безопасности Елены Скалозубовой из компании MONS (входит ГК «КОРУС Консалтинг»)**, которая недавно вышла на российский рынок информационной безопасности.

КУЛЬТУРА БЕЗОПАСНОСТИ: ОТ ТОП-МЕНЕДЖМЕНТА ДО РЯДОВЫХ СОТРУДНИКОВ

Один из ключевых трендов последних лет — смещение фокуса с исключительно технических мер защиты на формирование осознанной культуры безопасности во всей организации. Александр Шепилов подчеркивает, что роль директора по информационной безопасности в компании — это сочетание доверенного советника, регулятора и стратегического партнера. С каждым годом эта роль становится все более значимой, особенно в технологических компаниях, где ИБ становится неотъемлемой частью бизнес-процессов. Ключевым фактором успеха является включенность руководства и сотрудников.

В «Ростелекоме» культура безопасности развивается на уровне проектных команд и департаментов, так и благодаря личному участию руководителей подразделений. Это позволяет избегать формального подхода и повышает вовлеченность всех участников процесса.

По словам Александра Шепилова, благодаря такому подходу безопасность воспринимается как часть общей стратегии компании, руководители учитывают риски при планировании проектов, а ресурсы на обеспечение информационной безопасности расходуются более «точечно», исходя из реальных потребностей. В MONS, где команды ИБ часто работают с разными заказчиками, подход к управлению строится на доверии и проактивности.

> Мы сознательно культивируем принцип «ошибаться можно, бездействовать нельзя». Каждая ошибка — это повод для разбора и улучшений, а не для наказаний. Так мы формируем культуру осознанного отношения к информационной безопасности.
>
> Елена Скалозубова,
> Ведущий архитектор по информационной безопасности MONS (ГК «КОРУС Консалтинг»)

Оба эксперта, несмотря на разницу в масштабах организаций, сходятся в главном: без вовлеченности людей и поддержки руководства даже самые продвинутые технологии не дадут полноценного результата. Например, можно установить дорогостоящую систему защиты от утечек данных (DLP), но, если сотрудники продолжают пересылать конфиденциальные файлы через мессенджеры, риски останутся критически высокими. Это как приобрести самый безопасный автомобиль, но не пристегиваться ремнями — техническая защита есть, а реальной безопасности нет.

КОММУНИКАЦИЯ МЕЖДУ ИБ И БИЗНЕСОМ: КАК ПРЕОДОЛЕТЬ «ЭФФЕКТ ПОЛИЦЕЙСКОГО»?

Одна из ключевых проблем в области информационной безопасности — противоречия между интересами ИБ-подразделений и бизнеса. С одной стороны, требования безопасности диктуют необходимость ограничений и жесткого контроля, с другой — бизнес-процессы требуют гибкости и оперативности. Именно поэтому важно найти баланс и согласовать цели этих направлений.

В «Ростелекоме» этого удалось достичь за счет раннего подключения экспертов по ИБ к проектным командам. Такой подход позволяет сразу закладывать требования к безопасности на этапе проектирования решений, а не внедрять защитные меры постфактум.

> Мы выстроили систему взаимодействия между подразделениями, благодаря чему информационная безопасность интегрирована в ключевые бизнес-процессы с самого начала. Это повышает уровень доверия, позволяет оперативно реагировать на изменения и создает конкурентные преимущества для компании
>
> Александр Шепилов,
> Директор направления обеспечения ИБ корпоративных информационных систем, «Ростелеком»

Кроме того, сотрудники «Ростелекома» стали гораздо внимательнее относиться к рекомендациям специалистов по ИБ — во многом благодаря системной работе по информированию и развитию культуры безопасности. Стратегия MONS также подразумевает ставку на интеграцию ИБ в бизнес-процессы на самых ранних этапах проекта.

> Мы давно отказались от роли «надзирателей». Вместо этого мы объясняем требования к безопасности на языке бизнеса, показываем, как они помогают снижать реальные риски. Важно, чтобы ИБ-специалисты участвовали в проектах с самого начала, тогда безопасность становится естественной частью бизнес-процессов, а не тормозом. Например, вместо того чтобы просто запретить облачные хранилища, мы помогаем подобрать защищенные корпоративные аналоги и показываем, как утечка данных через «левые» сервисы может сорвать важную сделку или привести к штрафам
>
> Елена Скалозубова,
> Ведущий архитектор по информационной безопасности MONS (ГК «КОРУС Консалтинг»)

Таким образом информационная безопасность перестает быть «карательным» подразделением и становится стратегическим партнером бизнеса.

БАЛАНС МЕЖДУ ЗАЩИТОЙ И УДОБСТВОМ: ИСКУССТВО УПРАВЛЯЕМОГО РИСКА

ак обеспечить надежную защиту, не превращая рабочие процессы в «полосу препятствий»? Слишком жесткие ограничения снижают продуктивность, а слабая защита открывает двери для кибератак. Например, при внедрении многофакторной аутентификации для всех сервисов без исключения сотрудники могут тратить до 30% рабочего времени только на подтверждение входа. Однако если оставить простые пароли для «некритичных» систем, злоумышленники могут использовать их как лазейку для атак.

В «Ростелекоме» применяют системный подход к обеспечению безопасности, который учитывает степень критичности информационных активов для бизнес-процессов компании. При этом оценка значимости актива представляет собой комплексный многофакторный анализ.

Важно помнить, что даже на первый взгляд незначимый актив (например, сайт-визитка) при его компрометации может нанести серьезный репутационный ущерб. Поэтому в компании реализован непрерывный процесс достижения базового уровня защищенности для всех информационных активов.

MONS применяет риск-ориентированный подход, который позволяет находить оптимальный баланс.

> Мы всегда оцениваем, к каким последствиям может привести потенциальный инцидент, и подбираем меры защиты так, чтобы они минимально влияли на пользовательский опыт. Например, многофакторная аутентификация критически важна для доступа к финансовым системам, но может быть избыточной для внутреннего портала.
>
> Елена Скалозубова,
> Ведущий архитектор по информационной безопасности MONS (ГК «КОРУС Консалтинг»)

Универсальных решений здесь нет — системы информационной безопасности должны быть гибкими и отвечать реальным запросам бизнеса с точки зрения обеспечения ИБ.

АУДИТ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ: ОТ ФОРМАЛЬНОГО СООТВЕТСТВИЯ К РЕАЛЬНОЙ ЗАЩИТЕ

Слепое следование стандартам ИБ без учета реальных рисков напоминает покупку дорогого замка для стеклянной двери. Как правило, соблюдение стандартов — не бюрократическая формальность, а необходимость: они

аккумулируют проверенные отраслевые практики, помогают избежать базовых ошибок защиты, часто являются обязательными регуляторными требованиями и существенно снижают юридические риски компании. При этом соответствие стандартам — необходимое, но недостаточное условие.

Александр Шепилов отмечает, что в «Ростелекоме» уделяют особое внимание анализу и адаптации требований регуляторов.

> Необходимо сначала научиться однозначно понимать требования, а уже потом подбирать оптимальные способы их исполнения. Важно соблюдать баланс: выполнять требования их не для галочки, а максимально эффективно.
>
> Александр Шепилов,
> Директор направления обеспечения ИБ корпоративных информационных систем, «Ростелеком»

Со своей стороны Елена Скалозубова подчеркивает, что В MONS приоритезируют уязвимости, оценивая их по нескольким критериям:

Мы учитываем не только CVSS-баллы, но и критичность актива, вероятность эксплуатации уязвимости, доступность средств атаки. Это позволяет сосредоточиться на устранении действительно опасных угроз, а не тратить ресурсы на формальное закрытие всех пунктов чек-листа.

Елена Скалозубова,
Ведущий архитектор по информационной безопасности MONS (ГК «КОРУС Консалтинг»)

Оба подхода объединяет общий принцип: безопасность должна измеряться не количеством выполненных требований, а реальным снижением рисков.

БУДУЩЕЕ ИБ: ИИ, ЦЕПОЧКИ ПОСТАВОК И ZERO TRUST

Александр Шепилов и Елена Скалозубова выделяют три ключевых направления развития информационной безопасности, которые станут определяющими для компаний в ближайшие годы:

1. Безопасность как конкурентное преимущество

В условиях роста киберугроз внедрение принципов «security by design» с первых этапов разработки продуктов становится стратегическим фактором

успеха. Компании, инвестирующие в защищенные решения, не только снижают риски, но и укрепляют доверие клиентов и партнеров.

2. Импортозамещение и доверие к отечественным решениям

Переход на российские аналоги средств ИБ, соответствующие международным стандартам, позволяет снизить зависимость от иностранных поставщиков. Однако критически важны постоянная верификация и совершенствование таких решений для обеспечения стабильной защиты.

3. Культура кибергигиены

Повышение осведомленности сотрудников и пользователей об актуальных угрозах и методах защиты остается важным элементом безопасности. Системное обучение и развитие цифровой грамотности формируют устойчивость к атакам на уровне человеческого фактора.

Вместе с тем, эксперты прогнозируют усиление следующих угроз:

- Использование ИИ для генерации фишинга, промпт-инъекций и манипуляций с данными
- Атаки на цепочки поставок (supply chain), где злоумышленники атакуют уязвимых подрядчиков
- Риски для облачных сервисов и API, лежащих в основе цифровой трансформации
- Развитие ботнет-сетей за счет компрометации IoT-устройств

Подготовка к этим вызовам требует перехода к архитектуре Zero Trust, автоматизации мониторинга аномалий и жесткого контроля доступа для подрядчиков, поскольку современные киберугрозы становятся все более изощренными и комплексными, требуя принципиально новых подходов к защите. А компании, которые воспринимают безопасность не как обузу, а как конкурентное преимущество, получают не только защиту от угроз, но и фундамент для устойчивого развития.

Компании, которые рассматривают безопасность не как затраты, а как инвестиции в устойчивое развитие, получат не только защиту от угроз, но и значимое конкурентное преимущество на рынке.