**Управление Безопасностью в Организации**

**Политики Информационной Безопасности**

* Разработка и внедрение политик безопасности.

ольшинство крупных компаний в России не всегда готовы защитить свою безопасность в сфере информационного взаимодействия с другими организациями. Утечки информации, неосторожное поведение сотрудников, диффамация – все это подрывает конкурентоспособность компании. При разработке системы защиты необходимо опираться и на российские, и на международные стандарты. Это позволит и взаимодействовать с российскими государственными органами в соответствующем правовом поле, и успешно сотрудничать с зарубежными партнерами.

**Нормативы, используемые для разработки информационной безопасности**

Выбор нормативной базы, на которой строится разработка политики, зависит от того, в каком правовом поле и деловой среде преимущественно работает компания. Организации, привыкшие выстраивать свою деятельность на базе международных стандартов качества управления, ISO, будут готовы опираться в работе по подготовке политики информационной безопасности на такие нормативные акты, как ISO/IEC 27001-2005, ISO/IEC 17799-2005, ISO/IEC TR 13335. Российские предприятия, обеспечивающие обработку персональных данных или работающие со сведениями, содержащими государственную тайну, должны работать и с нормативами ГОСТ Р ИСО/МЭК 15408.

Разработанные на их базе системные программы охраны обрабатываемых массивов сведений помогут создать единую концепцию защиты от внешних и внутренних посягательств, в которой будут задействованы все уровни иерархии предприятия – от руководства и топ-менеджеров до линейных сотрудников. Включение каждого подразделения в работу на основе общей системы позволит полностью избежать пробелов в сфере обороны или конкуренции отдельных звеньев системы. Политика должна состоять из совокупности административных, организационных и технических мер, за каждую из которых должно отвечать отдельное подразделение. Некоторые процессы включают в себя последовательную работу нескольких служб, от согласованности которых зависит защита компании на сложном и конкурентном рынке. Прорыв в системе безопасности может причинить ущерб интересам и юридического лица, и его собственников, и сотрудников, чья профессиональная репутация может оказаться под угрозой, а персональные данные станут достоянием третьих лиц.

**Какой ущерб может причинить отсутствие политики безопасности**

Российское законодательство выделяет несколько видов массивов защищаемой информации, доступ к работе с которой имеют предприятия различной формы собственности и государственные органы. Среди них:

* коммерческая тайна, собственная и доверенная контрагентами;
* банковская тайна, сведения о счетах и вкладах граждан и предприятий;
* государственная тайна, доступ к которой могут получить многие участники тендеров на государственные закупки;
* персональные данные сотрудников и иных лиц, обрабатываемые различными операторами, как входящими в реестр, так и не входящими.

Утечка этих сведений с использованием любых каналов незаконного перехвата информации приводит к следующим видам ущерба:

* ухудшение деловой репутации компании;
* негативное воздействие регулятора;
* отзыв лицензии или иного допуска к сведениям, которые охраняются особым образом;
* потеря клиентов, снижение интенсивности денежного потока;
* потеря собственных разработок, маркетинговых исследований, приоритета при выпуске нового продукта;
* утрата влияния на рынке, отдельных секторов рынка;
* прямые иски о возмещении вреда, вызванного утратой коммерческой тайны контрагентов, или морального вреда.

Все эти риски в финансовом плане оцениваются очень высоко. Предприниматели должны приложить все силы к разработке и внедрению работающей системы защиты конфиденциальной информации, что в дальнейшем позволит защитить свои активы от серьезного ущерба.

Расходы на внедрение систем относятся, по правилам налогового учета, на снижение налога на прибыль, поэтому уровень затрат окажется разумным.

*К чему приводит неосмотрительное отношение к персональным данным?*[*Реальные кейсы.*](https://searchinform.ru/news/world-news/personalnye-dannye)

**Цели и задачи разработки политики информационной безопасности**

Не все предприятия понимают необходимость системного отношения к защите своих бизнес-интересов от утечек информации. Антивирусной защиты и обязания сотрудников своевременно менять пароли и не выносить из офиса документы должно хватить, по мнению руководства компаний, для обеспечения своей информационной неприкосновенности. Это не так, деятельность любой организации может представлять интерес для конкурентов, которые смогут использовать самые современные и нетривиальные способы проникновения в охраняемые базы данных. Это приводит к необходимости отказаться от разрозненных мер и опоры на деятельность служб безопасности и разработать политику, в которой будут предложены системные меры защиты.

Должны одновременно решаться такие задачи, как:

* выявление рисков, угрожающих всему периметру безопасности;
* внедрение средств защиты;
* расследование инцидентов информационной безопасности, зафиксированных случаев утечек;
* выявление виновников и привлечение их к ответственности с целью сохранения финансовых средств предприятия.

Если руководство не готово само проявить инициативу в подготовке такой политики, задача довести ее необходимость до топ-менеджеров ложится на плечи служб безопасности и IT-обеспечения. Документ должен утверждаться на уровне Совета директоров, если он присутствует в компании, расходы на внедрение политики информационной безопасности необходимо согласовывать с акционерами или собственниками, чтобы избежать обвинений в нецелевом расходовании средств.

Разработка политики безопасности связана с внедрением самых современных программных продуктов, стоимость которых может быть относительно высока. Каждое должностное лицо должно понимать необходимость внедряемых методов, программных продуктов, стандартов и соотносить расходы на их внедрение с фактическим увеличением стоимости компании. Наличие сертификации и аттестации по стандартам ISO/IEC 27001-2005 при оценке компании независимыми оценочными агентствами положительно повлияет на ее капитализацию.

Внедрение любой защитной меры всегда становится компромиссом между снижением уровня риска и удобством работы конкретного сотрудника, но дополнительные преимущества переведут целесообразность внедрения политики информационной безопасности на существенно более высокий уровень.

**Взаимодействие с пользователями**

На этапе разработки системы мер и ее внедрения лица, которым будет поручена эта задача, столкнутся с негативной реакцией большинства сотрудников IT-служб и других работников компании, которым придется отказаться от удобных стандартов работы. Та же бухгалтерия, которая не сможет больше сводить баланс вечером в домашних условиях, сочтет действия разработчиков опасными. От IT-служб, объем работы которых неминуемо увеличится, можно будет услышать критические реплики следующих типов:

* почему необходимо работать по нелогичной и ресурсозатратной схеме, а не по простой, быстрой и эффективной;
* почему на ненужные действия тратится столько средств и ресурсов компании;
* у нас нет ничего, что было бы интересно хакерам.

На все эти вопросы необходимо подготовить понятные и лаконичные ответы. Желательно, чтобы они были подкреплены утвержденной на высшем уровне политикой. Наличие при подготовке пояснительных записок и обоснований знаний о том, что конкуренты сталкивались с подобными ситуациями и в ряде случаев возбуждались даже уголовные дела, поможет сломить сопротивление. Оставшиеся имеют возможность готовить служебные записки на уровень высшего руководства.

**Этапы разработки политики информационной безопасности**

Не всегда компании готовы самостоятельно разработать политику информационной безопасности. Требуется привлечение экспертов, готовых предложить новейшие разработки. При этом эксперты должны ясно понимать, что их аудиторией являются Совет директоров и высший менеджмент компании, политика должна опираться на их интересы и полностью соответствовать им. Сопротивление может возникнуть на низовых уровнях, его нужно ожидать и подготовить достаточные меры, чтобы иметь возможность его сломить.

С учетом этих особенностей разработки сложного комплекса организационных и программно-технических мер процесс создания политики информационной безопасности будет состоять из следующих этапов:

* проведение аудита состояния информационной безопасности с использованием собственных ресурсов и привлеченных экспертов;
* анализ выявленных рисков, разработка, предложение и защита возможных сценариев построения систем обороны;
* разработка стандартов системы информационной безопасности, согласование их со всеми причастными службами;
* выбор оптимальных, экономически выгодных и внедряемых решений защиты информационной безопасности;
* разработка нормативно-правовой документации по обеспечению информационной безопасности, начиная от политик верхнего уровня и заканчивая стандартами работы с базами данных и компьютерной техникой;
* согласование и утверждение разработанных документов на уровнях советов директоров и исполнительного органа компании;
* внедрение документов, их апробация;
* сопровождение эффективной работы всех созданных секторов безопасности, доработка документов;
* проверка качества работы систем безопасности, их аудит и совершенствование.

Все эти этапы требуют внимательного отношения к любой процедуре, внедрение которой должно производиться с учетом мнения всех подразделений, согласования всех требуемых документов, в противном случае неизбежно возникновение конфликта интересов различных департаментов. Его наличие существенно затруднит работу компании.

**Структура политики информационной безопасности**

Процесс подготовки и согласования политики может занять до полугода, начиная от момента начала аудита, завершая этапом аттестации и сертификации системы. Разработанная и утвержденная документация должна включать в себя следующие разделы:

* перечисление объектов, в отношении которых устанавливается режим информационной безопасности, их ранжирование по значимости и требуемой степени защиты;
* описание функций каждого подразделения, ответственного за обработку данных и их защиту, описание самих функций системы информационной безопасности;
* описания технологий, применяемых для обеспечения сохранности информации;
* перечень действующих и потенциальных угроз информационной безопасности, описание степени их серьезности и реализуемости;
* модель вероятных проникновений сквозь контуры информационной безопасности;
* описание внешних и внутренних субъектов, которые могут стать источниками потенциальной угрозы;
* описание общих принципов и стандартов подходов к защите информационной безопасности, основанных на использовании разработок ISO/IEC 27001-2005 и действующего в этой сфере российского ГОСТа;
* описание применяемых административных мер, документов, стандартов;
* описание понятия инцидента информационной безопасности, процедур уведомления о его возникновении;
* описание применяемых организационных мер, действий сотрудников компании по обеспечению информационной безопасности;
* описание систем доступа ко всем информационным ресурсам организации, ранжирование систем доступа применительно к аппаратному обеспечению программных средств, базам данных. Доступ к информации должен быть ранжирован в зависимости от ранга сотрудника, его соответствия требованиям служб безопасности, важности охраняемых данных. Надо исключить несанкционированный доступ к базам данных неуполномоченных лиц;
* описание выбранной политики защиты от вирусных атак, программ-вредителей, возможных действий хакеров;
* описание системы резервного копирования важных данных, ее периодичности, моделей хранения – на дисках, на посторонних серверах;
* описание того, в каком порядке будут проводиться аварийные и восстановительные работы при повреждении аппаратной части в случае пожара, проблем с электросвязью или по иным причинам, повлекшим за собой гибель компьютеров, носителей информации или самих баз данных;
* описание порядка тестирования, согласования, аттестации (при наличии предусмотренной стандартами ISO/IEC 27001-2005 необходимости) и сертификации уполномоченными органами созданной системы на соответствие выбранным стандартам. Без соблюдения этих процедурных моментов не обойтись, так как аттестация созданных систем информационной безопасности по требованиям сохранности данных не только по ISO/IEC 27001-2005, но и ГОСТу, позволяет получить возможность работы с данными ограниченного доступа. От наличия сертификации часто зависит получение лицензии на обработку этих данных. Процесс сертификации дает возможность и работы в российском правовом поле, и взаимодействия с иностранными компаниями, заинтересованными в защищенности передаваемых ими российским партнерам сведений, являющихся коммерческой тайной;
* описание системы расследования инцидентов информационной безопасности, производимого собственными силами или с привлечением компетентных организаций или правоохранительных органов;
* план мероприятий по постоянному поддержанию готовности системы к работе, ее обновлению при изменении правил сертификации или степени значимости угроз.

Большинство из предложенных разделов должны иметь общий характер и отсылать к отдельным стандартам и регламентам. Документ должен быть понятен всем пользователям, работающим в компании, термины, понятные только узким специалистам, должны остаться в предназначенной для их внимания документации.

Несмотря на сложность и большой объем затронутых тем, нужно соблюдать следующие требования:

* лаконичность – документ на 150-200 страниц, составлять которые так любят корпоративные департаменты, прочитан не будет, а значит, не будет и выполняться;
* предоставление рекомендаций максимально простым и понятным языком – все шаги должны быть расписаны на уровне понимания простого администратора.

Все регламенты, содержащие последовательность процессов, уровни ответственности, графические схемы нужно вынести в приложения.

Возможно, имеет смысл подготовить трехуровневую систему документа:

1. Сама политика.
2. Положение о подразделениях и положение об информации, составляющей коммерческую тайну.
3. Регламенты и методики.

В качестве примера, как не всегда стоит готовить документы, может быть взята регламентационная документация АО «РТИ». Сотрудниками радиоинститута был подготовлен документ, состоящий из 45 страниц, насыщенных специальными терминами. Специфика его работы предполагает повышенное внимание к информационной безопасности, но не для всех это приемлемо. Изложение теоретических принципов и подходов не будет насущной необходимостью, но отнимет время на согласование и понимание. В противовес ему, аналогичный документ в ПО «Газпромбанк» занимает всего 11 страниц, простым и ясным языком там изложены все нормы, необходимые для понимания принципа работы политики информационной безопасности.

Помимо документального нужно учитывать и производственный, и территориальный, и кадровый факторы, каждый из которых определит специфику защитных мер. Создание системы и политики безопасности требует от разработчиков максимального учета особенностей работы каждого юридического лица, графиков, территорий, ресурсов. Ее создание должно гарантировать максимально высокую степень защиты, при этом оно и последующее поддержание работоспособности системы не должны повлечь за собой высоких финансовых затрат. Общая производительность труда не должна страдать от излишнего количества регламентов. Кроме этого, сертификация, аттестация и внедрение новых программных продуктов требуют существенного пересмотра бюджета, поэтому, если принято решение о разработке и внедрении системы мер и документов, необходимы своевременная подготовка сметы и бюджета и их согласование на уровне высшего руководства.

Традиционно в крупных компаниях планирование бюджета производится на уровне квартала и года, и согласовывать бюджет на внедрение политики необходимо исходя из того, что на это потребуется не менее двух кварталов.

Разработка современных программных продуктов, например DLP-систем и SIEM-систем, закрывающих все информационные каналы от несанкционированного съема данных, их внедрение и адаптация к потребностям каждого конкретного предприятия требуют не только финансовых, но и временных ресурсов. Поэтому от подразделений, отвечающих за подготовку политики, зависит своевременное планирование средств и согласование их привлечения.

Системная работа в области информационной безопасности, таким образом, требует внимания не только специальных подразделений, но и финансовых, и бухгалтерских служб, и руководства компании. При этом о целях разработки этой системы уведомляются все сотрудники, которые должны быть лично заинтересованы в успешности ее реализации. Помочь в этом могут системы мотивации, при использовании которых ключевые показатели эффективности труда будут связаны с соблюдением требований политики, ее успешным внедрением. Таким образом, в процесс оказываются вовлеченными еще и кадровые службы предприятия.

Задача в условиях крупного предприятия реализовать все этапы процесса внедрения политики информационной безопасности (от начальных моментов согласования до внедрения, сертификации и аттестации) становится крайне сложной. Но целесообразность этого решения должна помочь превозмочь все преграды.