Вопрос 1. Политика информационной безопасности

1. 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.

2. Ущерб из-за отсутствия 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. <1>

<1> Сёрчинформ Статья: Разработка политики информационной безопасности. М., 2018.

3. Состав и разработка политики безопасности

Политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. На практике политика безопасности трактуется несколько шире – как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. Результатом политики является **высокоуровневый документ**, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Данный документ представляет методологическую основу практических мер (процедур) по реализации ОБИ и содержит следующие группы сведений.

1. Основные положения информационной безопасности.
2. Область применения.
3. Цели и задачи обеспечения информационной безопасности.
4. Распределение ролей и ответственности.
5. Общие обязанности.

Политика информационной безопасности

Основные положения определяют важность ОБИ, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

Областью применения политики безопасности являются основные активы и подсистемы АС, подлежащие защите. Типовыми активами являются программно-аппаратное и информационное обеспечение АС, персонал, в отдельных случаях – информационная инфраструктура предприятия.

Цели, задачи, критерии ОБИ вытекают из функционального назначения предприятия. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности (оперативной готовности) подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т. д. Здесь указываются законы и правила организации, которые следует учитывать при проведении работ по ОБИ.

Типовыми целями могут быть следующие:

- обеспечение уровня безопасности, соответствующего нормативным документам предприятия;
- следование экономической целесообразности в выборе защитных мер;
- обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС;
- обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации;
- выработка планов восстановления после критических ситуаций и обеспечения непрерывности работы АС и др.

Если предприятие не является изолированным, цели и задачи рассматриваются в более широком контексте: должны быть оговорены вопросы безопасного взаимного влияния локальных и удаленных подсистем.

В рассматриваемом документе могут быть конкретизированы некоторые стратегические принципы безопасности (вытекающие из целей и задач ОБИ). Таковыми являются стратегии действий в случае нарушения политики безопасности предприятия и сторонних организаций, взаимодействия с внешними организациями, правоохранительными органами, прессой и др. В качестве примера можно привести две стратегии ответных действий на нарушение безопасности:

- «выследить и осудить», когда злоумышленнику позволяют продолжить действия с целью его компрометации и наказания (данную стратегию одобряют правоохранительные органы!);
- «защититься и продолжить», когда организация опасается за уязвимость информационных ресурсов и оказывает максимальное противодействие нарушению.

Защититься и продолжить	Выследить и осудить
s активы ИВС недостаточно защищены; s продолжительность вторжения сопряжена с финансовым риском; s неизвестен круг пользователей; s пользователи могут привлечь к ответственности организацию ИВС за нанесенный ущерб и др.	s ИВС хорошо защищена, имеются надежные средства резервирования; s наблюдаются повторяющиеся и частые атаки; s действия злоумышленника можно контролировать; s организация имеет положительный опыт работы с правоохранительными и правозащитными органами и др.

Критерии выбора ответных мер

Политика безопасности затрагивает всех пользователей компьютеров в организации. Поэтому важно решить так называемые политические вопросы наделения всех категорий пользователей соответствующими правами, привилегиями и обязанностями.

Для этого определяется круг лиц, имеющий доступ к подсистемам и сервисам АС. Для каждой категории пользователей описываются правильные и неправильные способы использования ресурсов – что запрещено и разрешено. Здесь специфицируются уровни и регламентация доступа различных групп пользователей. **Следует указать, какое из правил умолчания на использование ресурсов принято в организации, а именно:**

- что явно не запрещено, то разрешено;
- что явно не разрешено, то запрещено.

Одним из самых уязвимых мест в ОБИ является **распределение прав доступа**. В политике безопасности должна быть утверждена схема управления распределением прав доступа к сервисам – централизованная или децентрализованная, или иная. Должно быть четко определено, кто распоряжается правами доступа к сервисам и какими именно правами. Целесообразно детально описать практические процедуры наделения пользователей правами. Здесь следует указать должностных лиц, имеющих административные привилегии и пароли для определенных сервисов.

Права и обязанности пользователей определяются применительно к безопасному использованию подсистем и сервисов АС. При определении прав и обязанностей администраторов следует стремиться к некоторому балансу между правом пользователей на тайну и обязанностью администратора контролировать нарушения безопасности.

Важным элементом политики является **распределение ответственности**. Политика не может предусмотреть всего, однако, она должна для каждого вида проблем найти ответственного.

Обычно выделяются **несколько уровней ответственности**. На первом уровне каждый пользователь обязан работать в соответствии с политикой безопасности (защищать свой счет), подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях. Системные администраторы отвечают за защиту соответствующих информационно-вычислительных подсистем. Администраторы сетей должны обеспечивать реализацию организационно-технических мер, необходимых для проведения в жизнь политики безопасности АС. Руководители подразделений отвечают за доведение и контроль положений политики безопасности.

С практической точки зрения, **политику безопасности целесообразно разделить на несколько уровней.** Как правило, выделяют два-три уровня.

1) Верхний уровень носит общий характер и определяет политику организации в целом. Здесь основное внимание уделяется: порядку создания и пересмотра политики безопасности; целям, преследуемым организацией в области информационной безопасности; вопросам выделения и распределения ресурсов; принципам технической политики в области выбора методов и средств защиты информации; координированию мер безопасности; стратегическому планированию и контролю; внешним взаимодействиям и другим вопросам, имеющим общеорганизационный характер.

На указанном уровне формулируются главные цели в области информационной безопасности (определяются сферой деятельности предприятия): обеспечение конфиденциальности, целостности и/или доступности.

2) Средний уровень политики безопасности выделяют в случае структурной сложности организации либо при необходимости обозначить специфичные подсистемы организации. Это касается отношения к перспективным, еще не достаточно апробированным технологиям. Например, использование новых сервисов Internet, организация связи и обработка информации на домашних и портативных компьютерах, степень соблюдения положений компьютерного права и др. Кроме того, на среднем уровне политики безопасности могут быть выделены особо значимые контуры АС организации, например, обрабатывающие секретную или критически важную информацию.

За разработку и реализацию политики безопасности верхнего и среднего уровней отвечают руководитель службы безопасности, администраторы безопасности АС, администратор корпоративной сети.

3) Нижний уровень политики безопасности относится к конкретным службам или подразделениям организации и детализирует верхние уровни политики безопасности. Данный уровень необходим, когда вопросы безопасности конкретных подсистем требуют решения на управленческом, а не только на техническом уровне.

Понятно, что на данном уровне определяются конкретные цели, частные критерии и показатели информационной безопасности, определяются права конкретных групп пользователей, формулируются соответствующие условия доступа к информации и т. п. Здесь из конкретных целей выводятся (обычно формальные) правила безопасности, описывающие, кто, что и при каких условиях может делать или не может. Более детальные и формальные правила упростят внедрение системы и настройку средств ОБИ.

На этом уровне описываются механизмы защиты информации и используемые программно-технические средства для их реализации (в рамках, конечно, управленческого уровня, но не технического).

За политику безопасности нижнего уровня отвечают системные администраторы.

В рамках разработки политики безопасности проводится **анализ рисков** (risk analysis). Это делается с целью минимизации затрат на ОБИ. Напомним, что основной принцип безопасности – затраты на средства защиты не должны превышать стоимости защищаемых объектов. При этом если политика безопасности оформляется в виде высокоуровневого документа, описывающего общую стратегию, то **анализ рисков (как приложение) оформляется в виде списка активов, нуждающихся в защите.** <1>

<1> Гладких А. А., Дементьев В. Е. Учебное пособие "Базовые принципы информационной безопасности вычислительных сетей". Ульяновск, 2009.