

1 Цели, задачи, предпосылки и направления организационной и управленческой работы в сфере информационной безопасности

Под понятием «информационная безопасность» принято иметь в виду состояние (уровень) защищенности информационных ресурсов – информационных объектов и информационных систем от негативных воздействий (как случайных, так и осуществляемых преднамеренно), которые могут нанести ущерб самой информации и средствам ее передачи и обработки, а, следовательно, отрицательно отразиться на владельцах информационных ресурсов, государстве, обществе и других участниках процессов информационного обмена. Большинство современных информационных ресурсов, а также информационных систем практически не могут рассматриваться в отрыве от комплекса элементов (факторов), связанных с обеспечением информационной безопасности – угроз для информационных ресурсов, различных средств и мер защиты, барьеров для проникновения, а также уязвимостей в системах защиты информации.

Таким образом, под информационной безопасностью в более общем виде следует понимать совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются.

Понятие информационной безопасности неразрывно связано с рисками для информационных ресурсов, под которыми (рисками) понимается возможность (вероятность) нанесения ущерба информационным ресурсам, снижения уровня их защищенности. Риски могут иметь различную природу и характеристики; одной из основных классификаций рисков для информационной безопасности (так же, как и многих других рисков в экономике и управлении) является их разделение:

Тема 2.1 – Предпосылки и основные направления развития планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

- на системные риски: неуправляемые риски, связанные с той средой и технической инфраструктурой, в которой функционируют информационные системы;
- операционные риски: как правило, управляемые риски, связанные с особенностями использования определенных информационных систем, их технической реализации, применяемыми алгоритмами, аппаратными средствами и пр.

В качестве методической основы для детализированного анализа рисков в практической работе может быть использован ГОСТ Р 51275-2006 – «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». Все негативные воздействия на информационные активы, защиту от которых (воздействий) предполагает информационная безопасность, могут быть разделены на три основных вида:

- нарушение конфиденциальности информации;
- разрушение (утеря, необратимое изменение) информации;
- недоступность информационных ресурсов – возникновение ситуаций, когда пользователи (все или их часть) на некоторый период времени теряют возможность доступа к необходимым данным (или информационным системам).

Непосредственным источником рисков и негативных воздействий являются угрозы, под которыми понимаются потенциальные или реально возможные действия по отношению к информационным ресурсам, нарушающие информационную безопасность. Выделяется множество типов угроз и множество критериев для классификации угроз информационной безопасности. Одним из основных таких критериев является расположение источника нарушений к информационным ресурсам, в отношении которых осуществляется негативное воздействие. В соответствии с этим критерием нарушения могут быть разделены:

Тема 2.1 – Предпосылки и основные направления развития планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

- на обусловленные внутренними факторами (персоналом предприятия, работой собственных информационных систем);
- обусловленные внешними факторами (злоумышленниками, не имеющими непосредственного отношения к компании – владельцу информационных активов, природными факторами и пр.).

Другим важным критерием является наличие намерений осуществить нарушение. В соответствии с ним выделяют:

- целенаправленные воздействия (могут быть осуществлены как собственным персоналом, так и внешними противниками);
- случайные воздействия (ошибки пользователей и администраторов, сбои и случайные нарушения в работе оборудования, непредвиденные воздействия природных факторов).

Также можно выделить следующие классификации угроз:

- по объектам (персонал, материальные и финансовые средства, информация);
- по величине ущерба (предельный, значительный, незначительный);
- по вероятности возникновения (весьма вероятные, вероятные, маловероятные);
- по типу ущерба (моральный, материальный)

На практике основными наиболее распространенными способами нарушения информационной безопасности являются:

- получение несанкционированного доступа (в том числе и путем превышения прав при санкционированной работе с информационными системами) к определенным сведениям или массивам данных, распространение которых ограничено, с целью их изучения, копирования, распространения, незаконного использования и пр.;
- несанкционированное использование информационных ресурсов (ресурсов вычислительных и телекоммуникационных систем) с целью

Тема 2.1 – Предпосылки и основные направления развития планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

получения выгоды или нанесения ущерба (как тем системам, которые незаконно используются, так и третьим лицам);

- несанкционированная злонамеренная модификация (изменение) данных;

- кража денежных средств в электронных платежных системах и системах «клиент-банк», а также кража бездокументарных ценных бумаг и иные формы незаконного присвоения имущественных прав;

- вывод из строя (полный или частичный) программных и аппаратных средств обработки, передачи и хранения информации;

- осуществление атак типа «отказ в обслуживании» – DoS (в частности, в отношении серверов в сети Интернет);

- распространение вирусов и других вредоносных программ, осуществляющих различные негативные воздействия.

Современная практика использования информационных систем характеризуется большим количеством и постоянным ростом числа нарушений информационной безопасности. Одним из важных факторов этого является постоянно растущая доступность современных информационных технологий для преступников, а также постоянно растущая привлекательность информационных систем как потенциальных объектов нападения. Также важным обстоятельством является постоянное усложнение и рост разнообразия используемых информационных систем и, в частности, программных продуктов. С учетом того, что в среднем каждая тысяча строк программного кода может содержать от 5 до 15 ошибок, появление все большего числа различных уязвимостей, создающих угрозы для информационной безопасности, становится практически неизбежным.

При этом, рост многообразия возможных нарушений, увеличение их количества, увеличение сложности информационных технологий, постоянно возрастающая доступность компьютеров и телекоммуникационных средств

Тема 2.1 – Предпосылки и основные направления развития планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

для преступников объясняют рост потребности владельцев информационных ресурсов (предприятий, организаций, органов государственной власти и управления) в реализации систематических, всеобъемлющих мер по обеспечению информационной безопасности.

Отдельные процессы, процедуры, механизмы и инструменты защиты информации, используемые владельцами информационных ресурсов и информационных систем, могут быть направлены:

- на ограничение и разграничение доступа;
- информационное скрывание;
- введение избыточной информации и использование избыточных информационных систем (средств хранения, обработки и передачи информации);
- использование методов надежного хранения, преобразования и передачи информации;
- нормативно-административное побуждение и принуждение.

На практике современные технологии защиты информации основаны на различных базовых сервисах (таких, как аутентификация, обеспечение целостности, контроль доступа и пр.), и используют различные механизмы обеспечения безопасности (такие, как шифрование, цифровые подписи, управление маршрутизацией и пр.). Однако комплексность и массовость использования информационных технологий, их интеграция в повседневную деятельность предприятий, организаций, правительственных учреждений не позволяют решать задачи информационной безопасности только одними техническими средствами.

2 Структура управления информационной безопасностью

Во всем комплексе деятельности по защите информации одно из наиболее важных мест занимает организационно-управленческая деятельность – организационное обеспечение информационной безопасности, которое представляет собой одно из четырех основных направлений работы в общей системе мер в сфере информационной безопасности, включающей в себя также разработку специализированного программного обеспечения, изготовление и использование специальных аппаратных средств, и совершенствование криптографических (математических) методов защиты информации (рисунок 1).

Основными задачами организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности являются:

- обеспечение комплексности всех решений, реализуемых в процессе обеспечения информационной безопасности;
- обеспечение непрерывности и целостности процессов информационной безопасности;
- решение методических задач, лежащих в основе эффективного управления информационной безопасностью, таких, как вопросы управления рисками, экономическое моделирование и пр.;



Рисунок 1 – Структура деятельности в сфере информационной безопасности

Тема 2.1 – Предпосылки и основные направления развития планирования и управления
информационной безопасностью
(Планирование и управление информационной безопасностью)

– управление человеческими ресурсами и поведением персонала с учетом необходимости решения задач информационной безопасности.

Под комплексностью решения задач информационной безопасности подразумевается взаимоувязанное выявление всех значимых информационных объектов, а также существующих и потенциально возможных угроз. На основе этого анализа необходимо обеспечить исчерпывающе полное (комплексное) внедрение и применение средств защиты информации, которые в той или иной мере могли бы нейтрализовать все существенные угрозы на всех потенциально уязвимых участках прохождения информационных потоков в течение всех этапов жизненного цикла информационных систем и организационных процедур. Меры по нейтрализации рисков также должны быть реализованы в комплексе с другими механизмами, такими, как, например, страхование. Другими словами, задачей менеджмента является системное использование всех необходимых частных (узкоспециальных) технологий и решений для каждой конкретной ситуации таким образом, чтобы во всей системе мер по защите информационных ресурсов не осталось «узких мест» – уязвимых участков, через которые могут быть осуществлены нападения и в которых могут произойти непреднамеренные нарушения. Сложность такого рода задач связана с тем, что они предполагают по возможности исчерпывающий анализ, как всех информационных ресурсов, так и всех возможных сценариев нападения на них и последующий подбор наиболее подходящих средств защиты.

Непрерывность процессов обеспечения информационной безопасности предполагает выделение необходимых ресурсов и организацию выполнения необходимых функций по защите информации в течение всего времени функционирования информационных систем и выполнения бизнес-функций (в том числе и в режиме «24x7x365» в тех случаях, когда это необходимо).

Тема 2.1 – Предпосылки и основные направления развития планирования и управления
информационной безопасностью
(Планирование и управление информационной безопасностью)

Разработка, совершенствование и поддержание в актуальном состоянии методических основ управления информационной безопасностью включает в себя, главным образом, применение общих для многих сфер менеджмента концепций и теорий – таких как, например, математические модели оценки рисков или теория инвестиционного анализа – применительно к ресурсам, используемым для обеспечения информационной безопасности, и информационным процессам.

Управление человеческими ресурсами в рамках управления информационной безопасностью включает в себя комплекс задач, охватывающий все основные аспекты деятельности людей: отбор и допуск персонала для работы с определенными информационными ресурсами, обучение, контроль правильности выполнения обязанностей, создание необходимых условий для работы и пр.

При этом конкретная структура и состав всех основных задач управления и организации в сфере информационной безопасности, а также непосредственно используемые методы будут определяться как уровнем, на котором осуществляется управленческая и организационная деятельности, так и конкретными условиями, в которых функционируют информационные системы, нуждающиеся в защите. Настоящий курс основан на концепции разделения всего многообразия методов и задач организации и управления в сфере информационной безопасности на несколько основных уровней и дальнейшего представления организационно-управленческих методов для каждого из этих уровней.

Под организационным обеспечением и менеджментом в сфере информационной безопасности обычно принято понимать решение управленческих вопросов на уровне отдельных субъектов (предприятий, организаций) или групп таких субъектов (партнеров по бизнесу,

организаций, которые совместно решают определенные задачи, требующие защиты информации).

Однако сложность и комплексность современных проблем в сфере информационной безопасности, глобализация информационных взаимодействий требуют более полного и широкого понимания организационной работы и менеджмента в этой области.

В частности, по мере глобализации информационных взаимодействий, усложнения программных и аппаратных средств обработки информации, проникновения информационных технологий в повседневную деятельность всех организаций и жизнь большинства людей появилась необходимость в специальных организационных и управленческих усилиях, направленных не на обеспечение защищенности отдельных информационных активов, а на поддержание различных элементов информационной инфраструктуры, которая в той или иной мере работает на обеспечение информационной безопасности определенных сообществ (заранее не определенного множества пользователей информационных систем и владельцев информационных ресурсов).

Таким образом, с развитием информационных технологий и интенсификацией информационного обмена организационная и управленческая работа в сфере информационной безопасности оказывается направленной не только на собственно защиту определенных информационных ресурсов, но и на более «глобальный» объект – создание и развитие безопасной информационной инфраструктуры (в разных смыслах этого термина и с учетом различных его аспектов). На практике такая инфраструктура может включать в себя:

Тема 2.1 – Предпосылки и основные направления развития планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

- надежную инфраструктуру передачи информации и рынок услуг доступа к таким каналам связи;
- рынок программных и аппаратных средств, обеспечивающих защиту информации;
- систему подготовки, переподготовки и повышения квалификации специалистов в сфере информационной безопасности;
- общие правила использования информации, а также ее передачи, совместной эксплуатации информационных сетей (в том числе протоколы информационного обмена);
- систему обмена информацией и распространения знаний о существующих уязвимостях тех или иных информационных технологий, возможных угрозах информационной безопасности и способах их нейтрализации;
- законодательную и правоприменительную систему, обеспечивающую охрану имущественных и иных интересов всех участников информационного обмена и пр.

Потребность в целенаправленном развитии и поддержании такой инфраструктуры порождает необходимость в выработке специфичных организационных и управленческих приемов, как правило, не характерных для информационной безопасности в привычном («узком») ее понимании. Такое расширение сферы интересов менеджмента информационной безопасности объясняет причины, по которым необходимо разделять несколько относительно самостоятельных организационных уровней, характеризующихся специфическими задачами, подходами к решению этих задач и используемыми организационными методами:

Тема 2.1 – Предпосылки и основные направления развития планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

1) Уровень международных профессиональных объединений (как правило, неправительственных и некоммерческих), так или иначе связанных со сферой информационных технологий, телекоммуникаций и информационной безопасности.

2) Уровень крупных компаний, работающих в сфере информационных технологий и в значительной мере определяющих (прямо или косвенно) состояние информационной безопасности в сообществе пользователей информационных систем, а также влияющих на безопасность различных элементов информационной инфраструктуры.

3) Государственный уровень – уровень государственных и межправительственных организаций, так или иначе влияющих на жизнь общества, состояние правовой системы, развитие экономики и технологий.

4) Уровень отдельных компаний (предприятий и организаций) – сообщество пользователей информационных систем, так или иначе заинтересованных в собственной информационной безопасности и обеспечивающих защиту имеющихся у них информационных ресурсов собственными силами.

Также отдельно можно выделить дополнительный промежуточный уровень, включающий в себя консалтинговые и внедренческие компании, учебные центры (включая также сообщество специалистов, занимающихся консультациями, внедрениями и обучением в индивидуальном порядке), работающие в сфере информационной безопасности и действующие как связующее звено между различными организационными уровнями, а также представляющие интересы различных участников информационного взаимодействия.

Все эти составляющие образуют своеобразную организационную иерархию, представленную на рисунок 2.

Тема 2.1 – Предпосылки и основные направления развития планирования и управления
информационной безопасностью
(Планирование и управление информационной безопасностью)

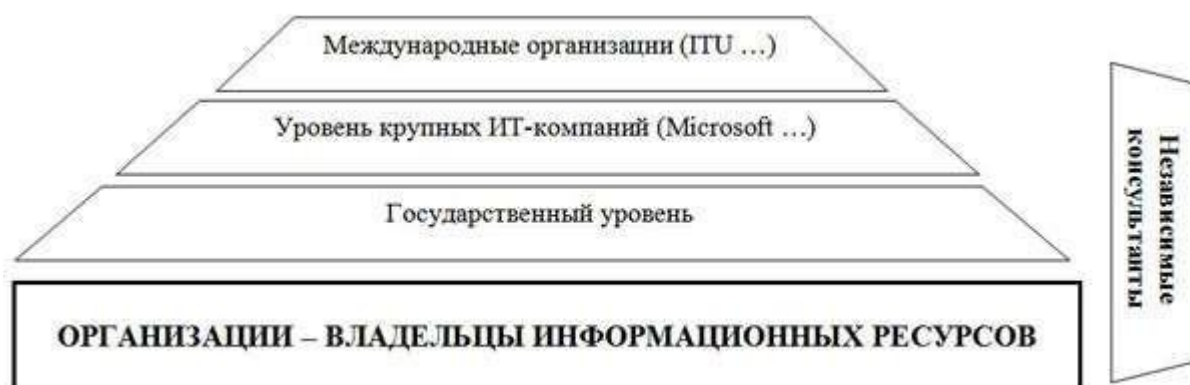


Рисунок 2 – Иерархия уровней организационной работы в сфере информационной безопасности

Следует понимать, что субъекты, находящиеся на верхних ступенях данной иерархии (в частности, государственные органы, крупные ИТ-корпорации), выступают не только как владельцы собственных информационных ресурсов, требующих защиты, но и как субъекты, которые воздействуют на инфраструктуру, лежащую в основе обмена и хранения информации, а также на общественно-экономические отношения, влияющие на информационную безопасность. И тот факт, что такие субъекты сами уделяют значительное внимание защите собственных ресурсов (вкладывают существенные средства в обеспечение информационной безопасности, инициируют новые разработки для собственных нужд, используют наиболее передовые технологии в этой сфере и пр.), не должен отвлекать внимание от того обстоятельства, что эти субъекты фактически создают инфраструктуру для повседневной деятельности множества компаний, организаций, людей, профессиональных и бизнес-сообществ и используют для этого организационные методы и приемы, которые существенно отличаются по своей природе от методов, характерных для работы по обеспечению информационной безопасности отдельных субъектов и защите отдельных информационных активов.

Тема 2.1 – Предпосылки и основные направления развития планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

Итак, необходимость самостоятельного рассмотрения субъектов, относящихся к верхнему уровню, с точки зрения организационного используют и методы, характерные для субъектов нижнего уровня представленной иерархии, т.к. являются владельцами собственных информационных ресурсов.

Представленное разделение на уровни должно быть основой для более целенаправленного развития системы менеджмента и налаживания взаимосвязей между различными уровнями организационной работы. Важность выделения и самостоятельного рассмотрения верхних уровней управленческой работы обусловлена тем, что целенаправленное осознание организационных вопросов, специфичных для верхних уровней иерархии, и их решение позволит более эффективно решать задачи развития национальных и региональных экономик в целом и отдельных отраслей (телекоммуникации, финансовые услуги и пр.), а не только решать задачи отдельных субъектов, участвующих в информационном обмене.

Основные особенности организационной работы на каждом из перечисленных уровней организации представлены в таблице 1.

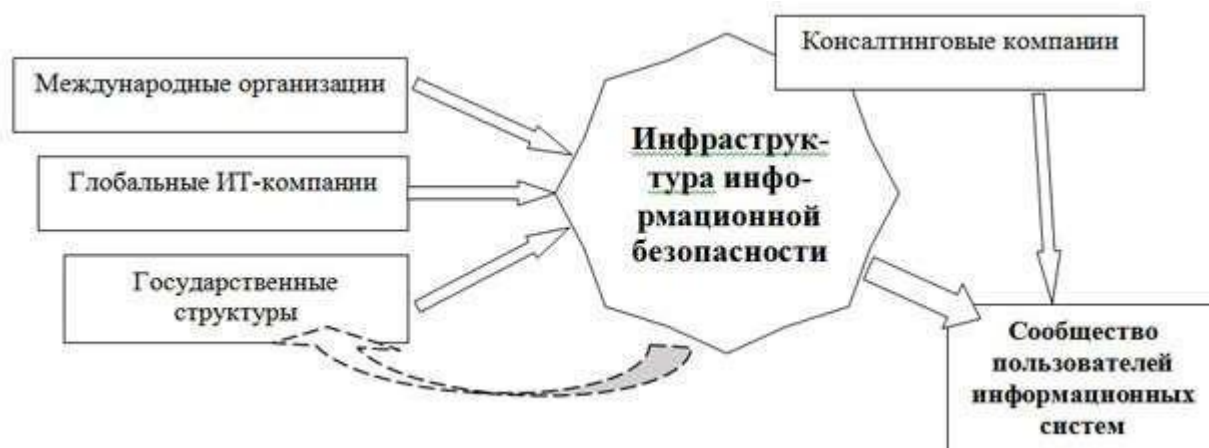


Рисунок 3 – Взаимосвязи уровней организации информационной безопасности

Тема 2.1 – Предпосылки и основные направления развития планирования и управления
информационной безопасностью
(Планирование и управление информационной безопасностью)

Таблица 1 и рисунок 3 наглядно демонстрируют причины, по которым каждый из уровней организационной работы в сфере информационной безопасности нуждается в индивидуальном подходе и применении специфичных методов организации и управления. В соответствии с этим разделением и строится структура настоящего курса, она включает в себя рассмотрение основных форм и приемов организации работы по обеспечению информационной безопасности на основных перечисленных уровнях:

- на уровне международных профессиональных организаций и бизнес-сообществ;
- на уровне крупных поставщиков технических (программных и аппаратных) средств обработки и передачи информации, имеющих влияние на состояние информационной безопасности большого числа предприятий, организаций и индивидуальных пользователей;
- на уровне государственных органов (в частности, правительств отдельных стран);
- на уровне отдельных предприятий, учреждений и организаций, являющихся непосредственными владельцами и пользователями информационных ресурсов.

Также рассматриваются вопросы работы специализированных компаний (консалтинговых, технологических, страховых), предоставляющих различные услуги, которые связаны с обеспечением информационной безопасности.

Тема 2.1 – Предпосылки и основные направления развития планирования и управления
информационной безопасностью
(Планирование и управление информационной безопасностью)

Таблица 1 – Задачи, роли и методы, используемые на различных уровнях
организационной работы в сфере информационной безопасности

| Организационный уровень | Основные задачи и роли | Основные специфичные методы организационной работы |
|---|---|---|
| Международные организации | Разработка правил и стандартов (в том числе и сетевых протоколов), имеющих глобальное значение. Обмен актуальной информацией и предупреждениями о новых угрозах | Координация работы специалистов, экспертов и исследователей, представляющих различные заинтересованные стороны |
| Глобальные ИТ- компании | Методологическая и организационная поддержка использования продуктов и услуг, поставляемых на рынок | Гибкое взаимодействие с клиентами (пользователями продуктов и услуг) с целью повышения эффективности использования информационных систем и получения отзывов для дальнейшего повышения качества поставляемых продуктов и услуг |
| Государственные организации | Регулирование использования информационных систем и распространения информации с целью недопущения противоправных действий, ущерба другим участникам информационного обмена, обществу и государственным органам | Разработка национальных и международных правил (законов, конвенций, соглашений и пр.), регулирующих отношения в информационной сфере; осуществление контроля (в различных формах). Осуществление правоприменительной и правоохранительной деятельности |
| Пользователи информационных систем – владельцы информации | Защита собственных информационных ресурсов | Выделение подразделений и специалистов, отвечающих за ИБ. Разработка и применение внутренних политик и правил безопасности |
| Консалтинговые и внедренческие компании, работающие в сфере ИБ | Выполнение некоторых функций ИБ на условиях аутсорсинга. Разработка и внедрение индивидуальных решений в сфере ИБ более эффективно, чем это могли бы сделать сами владельцы информационных ресурсов | Накопление и обобщение теоретических знаний и практических навыков с целью создания и внедрения организационных и технических решений в интересах клиентов |

1 Предпосылки развития государственного управления в сфере информационной безопасности

Основные задачи государственных органов в сфере информационной безопасности, также как и во многих других сферах, связаны с охраной общественных интересов, предотвращением противоправной деятельности, а также с защитой информации, имеющей государственную важность (военных сведений, информации о космических и ядерных технологиях и пр.). При этом решение вопросов информационной безопасности в частном секторе экономики, как правило, является прерогативой самих частных компаний и организаций, а вмешательство государства в эту сферу должно быть минимизировано. Таким образом, на практике деятельность органов власти, как правило, концентрируется на решении вопросов информационной безопасности внутри отдельных сфер, которые считаются наиболее важными для обеспечения государственной безопасности и достижения политических целей: вооруженные силы, внешняя разведка, стратегические технологии (например, космические, атомные и военные), государственные финансы, общественная стабильность и некоторые другие. Решению вопросов информационной безопасности в других областях государственными органами, как правило, уделяется меньше внимания. Государственные органы могут решать определенные задачи информационной безопасности, не относящиеся напрямую к защите государственных информационных систем, в тех случаях, когда выгоды от государственного вмешательства существенно превышают затраты и решения, предлагаемые государством, не составляют конкуренции альтернативным решениям (услугам, технологиям, методикам и пр.), которые предлагаются (или потенциально могут быть предложены) частными компаниями.

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

Деятельность государства в сфере информационной безопасности, как правило, строится на более общих задачах государственной власти, таких как:

- обеспечение социально-экономического развития страны и устойчивости финансовой системы;
- сохранение государственной и политической стабильности в стране;
- сохранение и развитие демократических институтов общества, а также обеспечение прав и свобод граждан;
- сохранение суверенитета государства;
- укрепление законности и правопорядка;
- участие в жизни международного сообщества.

По своей природе факторы, определяющие состояние информационной безопасности и, соответственно, деятельность государства в этой сфере, подразделяются на:

- организационно-технические;
- политические;
- социально-экономические.

Организационная деятельность государства в сфере информационной безопасности, как правило, сводится к противодействию различным угрозам:

1) Внешним, таким как деятельность иностранных спецслужб и вооруженных сил, враждебная экономическая и техническая политика отдельных государств, агрессивные рыночные стратегии крупных международных корпораций и финансово-промышленных групп, незаконная деятельность международных преступных и террористических группировок и пр.

2) Внутренним, таким как деятельность криминальных структур в сфере обращения информации, неправомерные действия государственных

структур, халатность или целенаправленные нарушения, допускаемые гражданами и организациями при использовании информационных систем и обращении информации, нарушения в работе информационных и телекоммуникационных систем и пр.

Таким образом, деятельность государства в этой сфере направлена на нейтрализацию существующих угроз информационной безопасности с учетом всех факторов, воздействующих как на сами управляющие государственные структуры, так и на информационные системы.

2 Общая методология и структура организационного обеспечения информационной безопасности на уровне государства

Для решения основных задач в сфере информационной безопасности действуют все основные органы государственной власти и управления: судебные, органы исполнительной власти, правоохранительные органы, организации и предприятия, которые контролируются государством и имеют доступ к информации, составляющей государственную тайну, и пр.

Для обеспечения информационной безопасности государственные органы выполняют следующие основные функции:

1) Выполняют судебные функции в отношении лиц, которые допустили правонарушения, связанные с использованием информационных ресурсов, и участвуют в хозяйственных спорах, связанных с нарушениями информационной безопасности.

2) Осуществляют правоприменительную деятельность, непосредственно реализуют меры по защите информационных ресурсов государственного управления, а также выполняют все функции, необходимые для реализации требований законодательства.

3) Создают законодательную базу, обеспечивающую защиту базовых прав частных лиц, предприятий и государства, таких как право на защиту частной информации, право на защиту коммерческой и банковской тайны,

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

право на беспрепятственный доступ к информации и пр. Данная функция осуществляется законодательными органами в сотрудничестве с органами исполнительной власти, общественными организациями, научно-исследовательскими учреждениями и другими заинтересованными участниками.

Функции создания и постоянного совершенствования законодательно-правовой базы, обеспечивающей защиту законных частных, коммерческих, общественных и государственных интересов, реализуются законодательными органами (парламентами) государств. Как правило, все законодательные функции в данной сфере в большинстве стран осуществляются центральными (федеральными) органами законодательной власти, а местные (региональные) органы таких полномочий не имеют. Для создания и поддержания в актуальном состоянии законодательства в сфере информационной безопасности в законодательных органах могут создаваться профильные комитеты и комиссии, которые состоят из членов данного законодательного органа, имеющих некоторые базовые знания и навыки в сфере информационных технологий и правового регулирования вопросов информационного обмена. Кроме того, вопросы совершенствования законодательства в сфере обеспечения информационной безопасности также могут решаться в различных профильных комитетах, подкомитетах и рабочих группах, специализирующихся на смежных проблемах государственного управления и социально-экономического регулирования, таких как:

- наука и образование;
- национальная безопасность;
- оборона;
- политика в сфере связи, информации и информатизации;
- промышленная и экономическая политика и пр.

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

Для разработки соответствующих нормативно-правовых актов подразделения (комитеты и подкомитеты) органов законодательной власти могут привлекать для совместной работы ответственных специалистов, руководителей, аналитиков и экспертов, работающих в:

- 1) Научно-исследовательских организациях, специализирующихся на соответствующих проблемах информационных технологий и управления.
- 2) Органах исполнительной власти (министерствах, отвечающих за научное и техническое развитие, т.н. «силовых» министерствах и ведомствах, юридических ведомствах и пр.).
- 3) Частных предприятиях, а также общественных и профессиональных организациях, которые занимаются оказанием информационных услуг, поставкой информационно-технических продуктов, специализирующихся на развитии информационных технологий и пр.

Процедуры согласования, принятия и утверждения законодательных актов, а также процедуры контроля за действиями органов исполнительной власти в каждой стране определяются в соответствии с действующим законодательством (конституцией).

Деятельность исполнительных органов государственной власти в сфере обеспечения информационной безопасности направлена на реализацию действующих в государстве законов и непосредственную защиту интересов государственной власти, гражданских прав и прав компаний, осуществляющих хозяйственную деятельность.

Конкретная работа органов исполнительной власти в сфере информационной безопасности, как правило, осуществляется по нескольким относительно самостоятельным направлениям:

- 1) Лицензирование и сертификация предприятий и организаций, занимающихся производством, продажей установкой и настройкой программных и аппаратных средств защиты информации.

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

2) Непосредственное осуществление функций защиты информации в государственных учреждениях и службах (правительство, вооруженные силы, органы внутренних дел и пр.).

3) Осуществление международного сотрудничества в сфере защиты информации (взаимодействие с правительствами и правоохранительными органами пр. стран) как в целях общего развития инфраструктуры информационной безопасности, так и для разрешения отдельных инцидентов (раскрытия преступлений и пр.).

4) Осуществление правоохранительной деятельности в сфере защиты информации (уголовного преследования лиц и преступных группировок, совершающих противоправные действия, содержащие признаки уголовных преступлений в соответствии с действующим уголовным законодательством).

5) Поддержка научных исследований в сфере информационной безопасности.

6) Поддержка образования и подготовки кадров, а также регулирование деятельности образовательных учреждений (включая установку образовательных стандартов).

7) Разработка государственных стандартов, относящихся к организации и технологиям защиты информации (программным и аппаратным средствам, средствам криптографии и пр.).

8) Установление конкретных правил производства, продажи, экспорта, импорта и использования средств защиты информации, а также организация системы контроля за соблюдением действующих законов и установленных правил.

Судебные функции, как правило, реализуются судами общей юрисдикции, так же, как и для всех остальных гражданских и уголовных дел. Специальных судебных инстанций, которые были бы предназначены для

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

рассмотрения дел, связанных с информационной безопасностью (таких как, например, суды по правам человека или военные суды), не существует. При этом могут создаваться судебные лаборатории, специализирующиеся на проведении экспертиз, анализов и исследований различных элементов информационных систем в связи с расследованиями и судебными разбирательствами по делам о нарушениях в сфере информационной безопасности.

Основой организации государственной деятельности в сфере информационной безопасности является национальная политика (доктрина, национальный план, национальная стратегия) информационной безопасности. Этот документ, издаваемый, как правило, главой исполнительной ветви власти (президентом страны) отражает:

- основные направления, в которых государство намерено осуществлять активные действия с целью повышения уровня информационной безопасности на национальном уровне (создание систем безопасности, упорядочивание взаимоотношений различных субъектов, пресечение правонарушений, развитие инфраструктуры и технологий безопасности и пр.):

- признание государственной властью существенной значимости проблем защиты информации для общества, личности, экономики и самого государства;

- современное понимание общего ландшафта информационной безопасности на национальном уровне: потенциально уязвимые информационные объекты, источники угроз и пр.

В рамках утвержденной государственной доктрины информационной безопасности:

- 1) Отдельные правительственные учреждения наделяются специфическими функциями и полномочиями, связанными с управлением

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

информационной безопасностью (как в общегосударственном масштабе, так и в рамках определенных сфер ответственности), а также создаются специальные структурные подразделения, отвечающие за решение вопросов защиты информации и информационной инфраструктуры.

2) Создается система локальных правовых актов, регулирующих отношения в сфере защиты информации, а также система государственных стандартов, относящихся к технологиям и организации защиты информации.

3) Создаются специализированные правительственные организации, отвечающие за реализацию политики информационной безопасности и решение отдельных задач в этой сфере.

Специализированные органы, создаваемые в структуре исполнительной власти для решения задач информационной безопасности на государственном уровне, как правило, подчиняются непосредственно главе исполнительной ветви власти, носят статус федеральных агентств, комитетов или комиссий и наделены правом самостоятельно издавать нормативные акты в рамках имеющихся полномочий, установленных действующим законодательством. Издаваемые таким образом локальные нормативные акты (указы, постановления, инструкции, порядки, правила и пр.) непосредственно регулируют отношения в сфере создания, распространения и использования средств автоматизации и защиты информации.

Государственная стандартизация технологий и методов, используемых в процессах защиты информации, осуществляется уполномоченными государственными органами с целью упорядочивания знаний о современном состоянии технологий и методов защиты и установления универсальных критериев надежности и функциональности для определенных технологий.

Государственная стандартизация позволяет достичь универсальности при оценке используемых технологий и методов и, таким образом, до

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

определенной степени упорядочить многие взаимоотношения, связанные с использованием таких технологий и методов.

Стандартизация, осуществляемая отдельными государственными органами, как правило, опирается на существующую систему имеющихся международных стандартов, а национальные органы, занимающиеся стандартизацией, могут принимать участие в разработке международных стандартов. Основными объектами государственной и международной стандартизации могут выступать:

- методы аутентификации;
- методы тестирования (проверки) и оценки информационных систем на предмет их защищенности;
- методы шифрования и криптографической защиты данных;
- некоторые другие элементы систем обеспечения информационной безопасности;
- технологии идентификации пользователей информационных систем.

3 Общая политика РФ в сфере информационной безопасности

Основой современной политики РФ в сфере информационной безопасности можно считать «Доктрину информационной безопасности РФ», утвержденную Президентом РФ В.В. Путиным 05.12. 2016 г. Этот документ:

- описывает основные направления международного сотрудничества в сфере информационной безопасности;
- описывает основные предпосылки формирования государственной политики в данной сфере (потребность в безопасности, существующие интересы, угрозы, источники угроз и пр.);
- описывает распределение ответственности между основными органами государственной власти, решающими задачи в сфере информационной безопасности;
- описывает состояние дел в сфере общегосударственного регулирования процессов информационной безопасности на момент утверждения Доктрины (основные достижения и недостатки);
- перечисляет основные информационные объекты (в различных сферах), на охрану которых должна быть направлена государственная политика;
- перечисляет основные организационные инструменты, используемые для реализации государственной политики и осуществления государственного управления в сфере информационной безопасности;
- перечисляет приоритетные направления деятельности государства (задачи, требующие безотлагательного решения) по обеспечению информационной безопасности;
- формулирует базовые задачи государства и общества, основанные непосредственно на необходимости выполнения требований Конституции, обеспечения суверенитета страны и пр.;

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

– формулирует основные методики, которые государство должно использовать для обеспечения информационной безопасности, а также специфику применения этих методов в отдельных областях общественной жизни.

В соответствии с Доктриной государство должно уделять внимание информационной безопасности в таких основных сферах, как:

- внешняя политика;
- внутренняя политика;
- духовная жизнь;
- информационные системы государственного управления;
- наука и техника;
- оборона;
- экономика.

К числу первоочередных мероприятий, которые должны быть реализованы на государственном уровне, Доктрина относит:

- подготовку кадров для работы в сфере информационной безопасности;
- принятие и реализацию федеральных программ, решающих определенные задачи информатизации и обеспечения информационной безопасности: создание информационных архивов и информационно-телекоммуникационных систем органов власти, развитие информационной культуры населения;
- разработку механизмов управления государственными средствами массовой информации и реализации государственной информационной политики;
- совершенствование законодательной базы в сфере информационных отношений;

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

– совершенствование и развитие системы государственных стандартов в сфере информатизации и обеспечения информационной безопасности и пр.

Как можно видеть из этого перечня, а также в целом из текста Доктрины, она предполагает определенное расширение понятия «информационная безопасность» и включение в него некоторых вопросов, которые связаны с деятельностью средств массовой информации и другими аспектами информационной политики, не имеющими прямого отношения к категории «информационная безопасность» в ее первоначальном понимании.

Помимо Доктрины также важным основополагающим документом, в значительной мере определяющим политику государства в сфере информатизации и обеспечения защиты информации, можно считать Федеральную целевую программу «Электронная Россия», реализация которой планируется в три этапа в период с 2002 по 2010 год. В частности, одной из заявленных целей реализации данной Программы является обеспечение реализации прав на «обеспечение конфиденциальности любой охраняемой законом информации, имеющейся в информационных системах». В целом предполагается, что весь комплекс мероприятий, предусмотренных Программой, должен обеспечить принципиально более высокий уровень надежности ключевых информационных потоков на государственном уровне.

Кроме того, важными организующими документами, действующими в этой сфере на государственном уровне, являются:

- 1) Федеральный Закон «О государственной тайне».
- 2) Федеральный Закон «Об информации, информационных технологиях и о защите информации».
- 3) Федеральный Закон «Об участии в международном информационном обмене».

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

Структура органов государственной власти, обеспечивающих информационную безопасность в РФ:

1) Важную роль в системе органов государственной власти, отвечающих за решение задач информационной безопасности, играет также Служба специальной связи и информации («Спецсвязь РФ»), с 2004 года входящая в состав Федеральной службы охраны.

2) Ведущим государственным учреждением, непосредственно ответственным за реализацию государственной политики в сфере информационной безопасности и защиту государственных интересов на общенациональном уровне, является Федеральная служба по техническому и экспортному контролю – ФСТЭК.

3) Основным государственным органом, определяющим политику РФ в сфере безопасности страны в целом и информационной безопасности в частности, является Совет безопасности РФ.

Вопросы повышения качества информационной работы и информационной безопасности решают также другие федеральные органы (в пределах своей компетенции):

1) Министерство внутренних дел РФ.

2) Министерство связи и массовых коммуникаций РФ;

Также отдельные государственные ведомства, предъявляющие особые требования к уровню защищенности информации, реализуют собственные мероприятия по обеспечению защиты информации:

1) ФСБ (Управление компьютерной и информационной безопасности, а также Центр по лицензированию, сертификации и защите государственной тайны, Управление специальной связи и НИИ информационных технологий);

2) Минатом РФ и система подведомственных ему предприятий (в составе которого функционирует Центр «Атомзащитаинформ»);

3) Центральный банк РФ (в составе которого функционирует Главное управление безопасности и защиты информации) и пр.

Совет Безопасности РФ, возглавляемый Президентом РФ, состоит из ключевых министров и рассматривает вопросы внутренней и внешней политики РФ в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности. Основными функциями Совета Безопасности являются:

- подготовка решений Президента РФ по соответствующим вопросам, в т.ч. по вопросам информационной безопасности;
- рассмотрение законопроектов, в рамках своей компетенции;
- организация и координация разработки стратегии в области внутренней, внешней и военной политики, военно-технического сотрудничества и информационной безопасности РФ;
- осуществление контроля за реализацией этой стратегии органами власти, оценка внутренних и внешних угроз жизненно важным интересам объектов безопасности и выявление их источников и пр.

Для решения задач, связанных с обеспечением информационной безопасности, в составе СБ функционирует созданное в 1997 году Управление информационной безопасности (одно из восьми профильных управлений), а также Межведомственная комиссия по информационной безопасности. Функциями Управления информационной безопасности являются:

- анализ и прогнозирование ситуации в области информационной безопасности РФ;
- выявление источников опасности, оценка внешних и внутренних угроз информационной безопасности и подготовка предложений Совету Безопасности по их предотвращению;

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

- подготовка предложений по проектам решений Совета Безопасности и информационно-аналитических материалов к его заседаниям по вопросам обеспечения информационной безопасности РФ;
- подготовка предложений Совету Безопасности по выработке и реализации основных направлений политики государства в области обеспечения информационной безопасности РФ;
- подготовка предложений Совету Безопасности по разработке проектов нормативных правовых актов, направленных на обеспечение информационной безопасности РФ;
- рассмотрение в установленном порядке проектов федеральных целевых программ, направленных на обеспечение информационной безопасности РФ, подготовка соответствующих предложений;
- участие в подготовке материалов по вопросам обеспечения информационной безопасности РФ для ежегодного послания Президента РФ Федеральному Собранию и для докладов Президента РФ.

Федеральная служба по техническому и экспортному контролю (ФСТЭК), до августа 2004 года известная как Государственная техническая комиссия при Президенте РФ (Гостехкомиссия РФ), была создана в январе 1992 года на базе Гостехкомиссии СССР по противодействию иностранным технологическим разведкам, которая, в свою очередь ведет отсчет своего существования с декабря 1973 года.

Произошедшее в 1992 году преобразование было связано со сменой политических приоритетов, интенсивным развитием электронных коммуникаций и средств вычислительной техники, отменой государственной монополии на многие сферы экономической и технической деятельности, развитием рыночных отношений, расширением международных связей и другими факторами. ФСТЭК, ранее подчинявшаяся напрямую Президенту РФ, в процессе административной реформы была подчинена Министерству

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

обороны. ФСТЭК является коллегиальным органом – в состав Коллегии входят около двадцати представителей различных министерств и ведомств (главным образом, в ранге заместителей министров и директоров департаментов), таких как МВД, МИД, ФСБ, Минатом, ФСО, СВР и пр.

Основными функциями ФСТЭК являются:

- организация и контроль за проведением работ по защите информации в органах государственного управления, объединениях, концернах, на предприятиях, в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от несанкционированного доступа к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения;
- поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации;
- проведение единой технической политики и координация работ по защите информации;

Для реализации функций по лицензированию в составе ФСТЭК функционируют 7 региональных управлений (по федеральным округам), а также 20 отраслевых аттестационных (лицензионных) центров.

Служба специальной связи и информации (Спецсвязь РФ), созданная в марте 2003 года в рамках Федеральной службы охраны на базе упраздненного Федерального агентства правительственной связи и информации (ФАПСИ), в целом призвана обеспечивать функционирование президентской связи, организацию, эксплуатацию и развитие специальной связи для государственных органов и решать другие аналогичные задачи.

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

При этом задачами Спецсвязи также являются:

- выполнение требований обеспечения информационной безопасности объектов государственной охраны;
- организация в системе специальной связи шифровальной деятельности, отнесенной к компетенции Спецсвязи РФ;
- организация и проведение мероприятий по предотвращению утечки по техническим каналам информации в системах специальной связи, информационно-технологических, информационно-аналитических и информационно-телекоммуникационных системах, находящихся в ведении Спецсвязи РФ;
- проведение работ по защите технических средств специальной связи, устанавливаемых в категорированных помещениях государственных органов, включая особо важные;
- участие в разработке и реализации мер по обеспечению информационной безопасности Российской Федерации, защите сведений, составляющих государственную тайну;
- участие в разработке нормативной технической документации по вопросам защиты информации в системах специальной связи;
- участие в создании, обеспечении и развитии системы электронного документооборота государственных органов с использованием удостоверяющих центров.

Министерство связи и массовых коммуникаций РФ в лице подчиняющегося ему Федерального агентства по информационным технологиям (Росинформтехнологии) осуществляет и организует следующие виды работ в сфере информационной безопасности:

- ведение единого государственного реестра сертификатов ключей подписей удостоверяющих центров и реестра сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, а также

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

обеспечение доступа к ним граждан, организаций, органов государственной власти и органов местного самоуправления;

- выполнение функции государственного заказчика научно-технических и инвестиционных программ и проектов в сфере информационных технологий;

- подтверждение подлинности электронных подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей.

Уполномоченным органом по ведению реестра доверенных удостоверяющих центров является ФГУП НИИ «Восход».

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных. В полномочия данного органа входит пресечение нарушений, которые могут возникать при обработке персональных данных граждан РФ.

В системе законодательной власти основным структурным подразделением, призванным решать вопросы формирования и реализации государственной политики в сфере информационной безопасности, является Комитет по безопасности Государственной думы Федерального собрания Российской Федерации. В составе этого Комитета функционирует Подкомитет по информационной безопасности. В законодательной работе в рамках этого Комитета принимают участие:

- представители ведущих научно-исследовательских учреждений и учебных заведений;

- представители крупных коммерческих компаний – лидеров в развитии организации и технологий информационной безопасности (в том числе банков, технологических компаний и пр.);

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

- представители общественных организаций, фондов и профессиональных объединений;
- руководители Совета безопасности РФ и пр. правительственных органов;
- специалисты и руководители профильных подразделений ФСБ, СВР, ФСТЭК, МВД и пр. ведомств.

1 Предпосылки к управлению информационной безопасностью предприятия

Обеспечение собственной информационной безопасности на предприятиях, как правило, является неотъемлемой частью общей системы управления, необходимой для достижения уставных целей и задач. Значимость систематической целенаправленной деятельности по обеспечению информационной безопасности становится тем более высокой, чем выше степень автоматизации бизнес-процессов предприятия и чем больше «интеллектуальная составляющая» в его конечном продукте, т.е. чем в большей степени успешность деятельности зависит от наличия и сохранения определенной информации (технологий, ноу-хау, коммерческих баз данных, маркетинговой информации, результатов научных исследований и пр.), обеспечения ее конфиденциальности и доступности для владельцев и пользователей. Роль информации и, в частности, т.н. «знаниевых активов» в деятельности предприятий возрастает по мере либерализации мировых рынков, когда материальные активы во все меньшей степени являются источниками конкурентных преимуществ в силу значительного уменьшения торговых барьеров. Нематериальные активы, существующие обычно в виде информации, в этих условиях начинают играть роль одной из ведущих основ для повышения конкурентоспособности и развития бизнеса.

Обеспечение информационной безопасности также, как правило, имеет большое значение не только для стратегического развития предприятия и создания основного продукта, но и для отдельных (иногда вспомогательных) направлений деятельности и бизнес-процессов, таких как коммерческие переговоры и условия контрактов, ценовая политика и пр.

Кроме того, значимость обеспечения информационной безопасности в некоторых случаях может определяться наличием в общей системе информационных потоков предприятия сведений, составляющих не только коммерческую, но и государственную тайну, а также другие виды

конфиденциальной информации (сведения, составляющие банковскую тайну, врачебную тайну, интеллектуальную собственность компаний-партнеров и пр.). Обеспечение информационной безопасности в этой сфере и, в частности, основные требования, организационные правила и процедуры непосредственно регламентируются федеральным законодательством, и надзор за выполнением требований осуществляется федеральными органами власти:

1) Для сведений, составляющих государственную тайну – Федеральный закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне» и связанные с ним подзаконные акты.

2) Для сведений, составляющих банковскую тайну – Федеральный закон «О банках и банковской деятельности» и связанные с ним смежные законы и подзаконные акты.

3) Для сведений, составляющих врачебную тайну – Основы законодательства РФ «Об охране здоровья граждан» (ст.61) и Закон РФ «О трансплантации органов и (или) тканей человека» (ст.14).

4) Для сведений, относящихся к некоторым другим видам тайны, таких как военная тайна, нотариальная тайна, адвокатская тайна, тайна страхования, тайна усыновления, налоговая тайна, тайна следствия и судопроизводства и пр.

Соответственно, лица, нарушающие требования информационной безопасности, могут быть не только подвергнуты дисциплинарным взысканиям, но и подлежат уголовному и административному преследованию.

Так же, как и на государственном уровне, управление информационной безопасностью на уровне предприятий направлено на нейтрализацию различных видов угроз:

– внешних, таких как неправомерные действия государственных органов (в том числе и зарубежных), противоправная деятельность преступников и преступных группировок, незаконные действия компаний-конкурентов и других хозяйствующих субъектов, недобросовестные действия компаний-партнеров, несоответствие действующей нормативно-правовой базы фактическому развитию технологий и общественных отношений, сбои и нарушения в работе

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)

глобальных информационных и телекоммуникационных систем и информационных систем компаний-партнеров (контрагентов) и пр.;

– внутренних, таких как ошибки и халатность персонала предприятия, а также намеренно допускаемые нарушения, сбои и нарушения в работе собственных информационных систем и пр.

Таким образом, управление информационной безопасностью на каждом отдельном предприятии должно осуществляться в контексте его общей хозяйственной деятельности: с учетом характера деятельности компании (технологии производства, специфики рынков сбыта и пр.), а также фактически складывающейся ситуации в рыночной конкурентной борьбе, государственной политике, развития правовой и правоохранительной системы, уровня развития отдельных используемых информационных и телекоммуникационных технологий и других факторов, формирующих общие условия текущей деятельности.

Формальным основанием (предпосылкой) для осуществления целенаправленной деятельности в сфере защиты информации, помимо общегосударственных требований к защите информации, составляющей государственную, военную, врачебную и банковскую тайну, также является перечень сведений, составляющих коммерческую тайну предприятия, который определяется предприятием самостоятельно с учетом требований действующего законодательства.

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)



Рисунок 1 – Предпосылки разработки политики безопасности предприятия

Кроме того, необходимость разработки и внедрения политики информационной безопасности может быть обусловлена такими обстоятельствами, как:

- необходимость уменьшения стоимости страхования информационных рисков или определенных бизнес-рисков;
- необходимость внедрения международных стандартов, таких как ISO 17799 или BS 7799.

Предпосылки разработки политики безопасности предприятия представлены на рисунке 1.

2 Структура управления информационной безопасностью предприятия

Для нейтрализации существующих угроз и обеспечения информационной безопасности предприятия организуют систему менеджмента в сфере информационной безопасности, в рамках которой (системы) проводят работу по нескольким направлениям:

- формирование и практическая реализация комплексной многоуровневой политики информационной безопасности предприятия и системы внутренних требований, норм и правил;
- организация департамента (службы, отдела) информационной безопасности;

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)

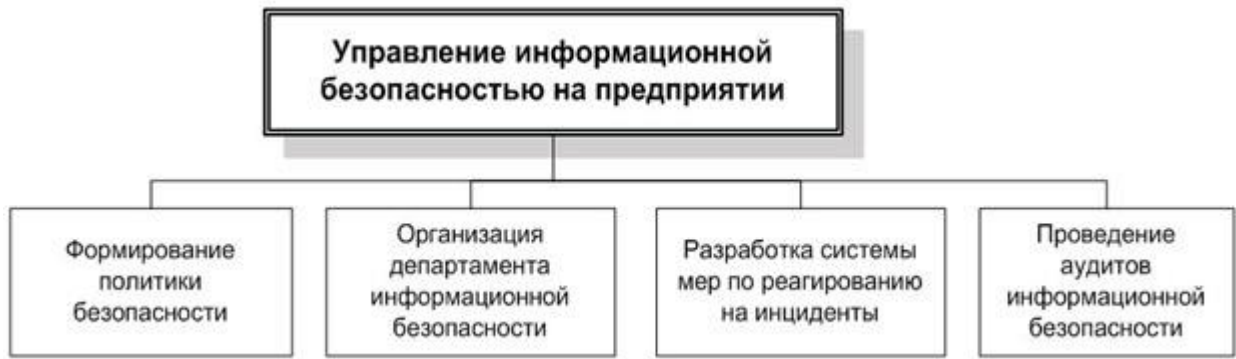


Рисунок 2 – Структура управления информационной безопасностью предприятия

- разработка системы мер и действий на случай возникновения непредвиденных ситуаций («Управление инцидентами»);
- проведение аудитов (комплексных проверок) состояния информационной безопасности на предприятии.

Каждое из этих направлений организационной работы имеет свои особенности и должно реализовываться с использованием специфических методов менеджмента и в соответствии со своими правилами. Политики и правила информационной безопасности являются организационными документами, регулирующими деятельность всей организации или отдельных подразделений (категорий сотрудников) в части обращения с информационными системами и информационными потоками. Департамент информационной безопасности является узкоспециализированным подразделением, решающим специфические вопросы защиты информации.

Система мер по реагированию на инциденты обеспечивает готовность всей организации (включая Департамент информационной безопасности) к осмысленным целенаправленным действиям в случае каких-либо происшествий, связанных с информационной безопасностью. Проведение внутренних аудитов информационной безопасности (периодических или связанных с определенными событиями) должно обеспечить контроль за текущим состоянием системы мер по защите информации и, в частности, независимую проверку соответствия реального положения дел установленным правилам и требованиям.

При этом каждое из направлений деятельности должно постоянно совершенствоваться по мере развития организации, а конкретные задачи должны постоянно уточняться в соответствии с изменением в организационной структуре, производственных процессах или внешней среде. Так, например, если предприятие начинает выпуск продукции военного назначения параллельно с выпуском гражданской продукции, то это может потребовать изменений всех основных направлений организационной работы в сфере обеспечения информационной безопасности:

- корректировки стратегии и основных положений политики информационной безопасности (на всех ее уровнях);
- изменения организационной структуры и функциональных задач департамента информационной безопасности;
- совершенствования системы реагирования на инциденты;
- использование более совершенных методик проведения аудитов информационной безопасности.

Структура управления информационной безопасностью предприятия представлена на рисунке 2.

3 Политика информационной безопасности предприятия

3.1 Структура политики информационной безопасности и процесс ее разработки.

Политика информационной безопасности представляет собой комплекс документов, отражающих все основные требования к обеспечению защиты информации и направления работы предприятия в этой сфере. При построении политики безопасности можно условно выделить три ее основных уровня: верхний, средний и нижний.

Верхний уровень политики информационной безопасности предприятия служит:

- для формулирования и демонстрации отношения руководства предприятия к вопросам информационной безопасности и отражения общих целей всего предприятия в этой области;
- основой для разработки индивидуальных политик безопасности (на более низких уровнях), правил и инструкций, регулирующих отдельные вопросы;
- средством информирования персонала предприятия об основных задачах и приоритетах предприятия в сфере информационной безопасности.

Политики информационной безопасности среднего уровня определяют отношение предприятия (руководства предприятия) к определенным аспектам его деятельности и функционирования информационных систем:

- отношение и требования (более детально по сравнению с политикой верхнего уровня) предприятия к отдельным информационным потокам и информационным системам, обслуживающим различные сферы деятельности, степень их важности и конфиденциальности, а также требования к надежности (например, в отношении финансовой информации, а также информационных систем и персонала, которые относятся к ней);
- отношение и требования к определенным информационным и телекоммуникационным технологиям, методам и подходам к обработке информации и построения информационных систем;
- отношение и требования к сотрудникам предприятия как к участникам процессов обработки информации, от которых напрямую зависит эффективность многих процессов и защищенность информационных ресурсов, а также основные направления и методы воздействия на персонал с целью повышения информационной безопасности.

Политики безопасности на самом низком уровне относятся к отдельным элементам информационных систем и участкам обработки и хранения

информации и описывают конкретные процедуры и документы, связанные с обеспечением информационной безопасности.

Разработка политики безопасности предполагает осуществление ряда предварительных шагов:

- оценку личного (субъективного) отношения к рискам предприятия его собственников и менеджеров, ответственных за функционирование и результативность работы предприятия в целом или отдельные направления его деятельности;
- анализ потенциально уязвимых информационных объектов;
- выявление угроз для значимых информационных объектов (сведений, информационных систем, процессов обработки информации) и оценку соответствующих рисков.

Осуществление предварительных шагов (анализа) позволяет определить, насколько информационная безопасность в целом важна для устойчивого осуществления основной деятельности предприятия, его экономической безопасности. На основе этого анализа с учетом оценок менеджеров и собственников определяются конкретные направления работы по обеспечению информационной безопасности. При этом в некоторых случаях личное мнение отдельных руководителей может и не иметь решающего значения. Например, в том случае, когда в распоряжении компании имеются сведения, содержащие государственную, врачебную, банковскую или военную тайну, основные процедуры обращения информации определяются федеральным законодательством, а также директивами и инструкциями тех федеральных органов, в чьей компетенции находятся вопросы обращения такой информации.

Таким образом, политика информационной безопасности (практически на всех уровнях) в части работы с такими данными будет основана на общих строго формализованных правилах, процедурах и требованиях (таких, как использование сертифицированного оборудования и программного

обеспечения, прохождение процедур допуска, оборудование специальных помещений для хранения информации и пр.).

При разработке политик безопасности всех уровней необходимо придерживаться следующих основных правил.

1) Политики безопасности на более низких уровнях должны полностью подчиняться соответствующей политике верхнего уровня, а также действующему законодательству и требованиям государственных органов.

2) Текст политики безопасности должен содержать только четкие и однозначные формулировки, не допускающие двойного толкования.

3) Текст политики безопасности должен быть доступен для понимания тех сотрудников, которым он адресован.

В целом политика информационной безопасности должна давать ясное представление о требуемом поведении пользователей, администраторов и других специалистов при внедрении и использовании информационных систем и средств защиты информации, а также при осуществлении информационного обмена и выполнении операций по обработке информации. Кроме того, из политики безопасности, если она относится к определенной технологии и/или методологии защиты информации, должны быть понятны основные принципы работы этой технологии. Важной функцией политики безопасности является четкое разграничение ответственностей в процедурах информационного обмена: все заинтересованные лица должны ясно осознавать границы, как своей ответственности, так и ответственности других участников соответствующих процедур и процессов. Также одной из задач политики безопасности является защита не только информации и информационных систем, но и защита самих пользователей (сотрудников предприятия и его клиентов и контрагентов).



Рисунок 3 – Жизненный цикл политики ИБ предприятия

Общий жизненный цикл политики информационной безопасности включает в себя ряд основных шагов:

- 1) Проведение предварительного исследования состояния информационной безопасности.
- 2) Собственно, разработку политики безопасности.
- 3) Внедрение разработанных политик безопасности.
- 4) Анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию (возврат к первому этапу, на новый цикл совершенствования).

Этот цикл (Рисунок 3) может повторяться несколько раз с целью совершенствования организационных мер в сфере защиты информации и устранения выявляемых недоработок.

3.2 Политика информационной безопасности предприятия – верхний уровень

Политика информационной безопасности верхнего уровня фактически является декларацией руководителей и/или собственников предприятия о необходимости вести целенаправленную работу по защите информационных ресурсов, что должно стать основой для более успешного функционирования предприятия в основном направлении его деятельности, а также устранить различные риски, которые могут привести к финансовым потерям, ущербу для репутации предприятия, административному и уголовному преследованию руководителей и другим негативным последствиям.

Политика информационной безопасности на этом уровне может определять и описывать:

- собственно, решение об осуществлении целенаправленной систематической деятельности по обеспечению информационной безопасности предприятия;
- перечень основных информационных ресурсов, таких как информационные системы, массивы данных, информация об отдельных фактах и явлениях (конструкторских разработках, коммерческих сделках, результатах НИОКР и пр.), защита которых имеет наибольший приоритет для всего предприятия;
- общий подход к распределению ответственности за обеспечение информационной безопасности внутри организации;
- указание на необходимость для всего персонала соблюдать определенные меры предосторожности при работе с информацией и информационными системами, повышать свою квалификацию в данной области и осознавать меру ответственности за возможные нарушения;
- отношение руководства предприятия к фактам нарушения требований по обеспечению информационной безопасности и лицам, совершающим такие

нарушения, а также общий подход к их преследованию в случае выявления таких фактов.

Одной из задач политики верхнего уровня является формулирование и демонстрация того, что защита информации является одним из ключевых механизмов обеспечения конкурентоспособности предприятия и обуславливает, как его способность достигать поставленные цели, так иногда и способность выживания и сохранения возможности продолжать деятельность. Для этого могут быть обозначены приоритетные направления хозяйственной деятельности и соответствующие им информационные системы и потоки информации, описана причинно-следственная связь между возможными нарушениями конфиденциальности и/или нарушениями в стабильной работе информационных систем, с одной стороны, и нарушениями нормального хода текущих хозяйственных операций, с другой стороны. На основе этого могут быть определены приоритетные направления деятельности по обеспечению информационной безопасности. В наибольшей степени зависимость общей эффективности деятельности от информационной безопасности характерна для таких компаний, которые:

- занимаются т.н. электронной коммерцией или работают в смежных сферах (электронные платежи, Интернет-реклама и пр.);
- непосредственно связаны с оборотом (созданием, куплей-продажей, охраной, оценкой) объектов интеллектуальной собственности и, в частности, наукоемких технологий;
- непосредственно связаны с обращением больших объемов информации, составляющей тайну других лиц (банки, медицинские учреждения, аудиторские компании и пр.).

При этом работа над политикой информационной безопасности должна включать в себя не только ее начальную разработку, но и постоянный мониторинг угроз, изменений во внешней среде для последующего уточнения

(или даже полной переработки) политики в соответствии с изменившимися условиями работы.

3.3 Политика информационной безопасности предприятия – средний уровень

Политики информационной безопасности среднего уровня непосредственно детализируют требования, задачи и правила, обозначенные в политике верхнего уровня, и отдельно описывают основные сферы, в которых необходимо системное осуществление тех или иных организационных и/или технических мероприятий.

Политика информационной безопасности среднего уровня должна содержать следующие основные разделы.

1) Общее описание той сферы деятельности (информационной технологии, аспекта информационной системы, бизнес-процессов предприятия), на которую она распространяется.

2) Область применения политики безопасности – перечень всех лиц, организаций, информационных систем, к которым она применяется или которые исключаются из сферы ее применения.

3) Непосредственное отношение предприятия к данному аспекту информационных технологий и информационной безопасности – основная часть политики безопасности, определяющая конкретные правила, критерии и требования к процедурам обращения информации, элементам информационной инфраструктуры, программным и аппаратным средствам и пр.

4) Распределение ролей и функций, необходимых для разрешения конкретных вопросов – закрепление за определенными сотрудниками (специалистами, руководителями) обязанностей по выполнению необходимой работы с целью решения задач в рамках данной политики безопасности.

5) Порядок разрешения возникающих вопросов – основные процедуры разрешения появляющихся затруднений в текущей работе и принятия решений о возможных исключениях из общих правил, а также перечень лиц

(подразделений), ответственных за непосредственную работу с персоналом предприятия по вопросам, относящимся к данной политике безопасности.

Одной из основ для реализации мероприятий в сфере информационной безопасности и детальной разработки политики безопасности является укрупненная классификация информационных ресурсов, имеющихся у предприятия. Все имеющиеся у предприятия информационные объекты (и соответствующие элементы информационной инфраструктуры), как правило, могут быть разделены на пять или шесть основных групп по уровню своей значимости и конфиденциальности.

1) Критически важная (абсолютно секретная) информация – информация, требующая особых гарантий безопасности.

2) Важная информация (информация, составляющая коммерческую тайну) – информация, используемая только внутри предприятия, нарушение конфиденциальности которой может нанести серьезный ущерб самому предприятию или его партнерам.

3) Значимая (конфиденциальная) информация – информация, предназначенная для использования ограниченным кругом сотрудников и руководителей предприятия.

4) Персональная информация – информация о сотрудниках, не подлежащая разглашению.

5) Информация для внутреннего использования – информация для использования внутри предприятия, нарушение конфиденциальности которой не может нанести вреда.

6) Прочая информация – открытая информация, конфиденциальность которой не имеет особого значения для деятельности предприятия.

Во всем объеме политик среднего уровня необходимо выделить два их основных вида.

1) Политики, относящиеся к определенным сферам деятельности предприятия и соответствующим информационным потокам (финансам, коммерческой деятельности и пр.).

2) Политики, относящиеся к определенным аспектам использования информационных технологий, организации информационных потоков и организации работы персонала на всем предприятии – вне зависимости от той сферы, где используются эти технологии или занят персонал.

К политикам первого типа могут относиться:

- политики обращения с информацией, составляющей государственную тайну;
- политики обращения с результатами НИОКР, конструкторской и технологической документацией, составляющей «ноу-хау» предприятия или его партнеров и пр.

Политики безопасности такого типа уточняют и дополняют общие для всего предприятия правила, распространяющиеся на все остальные информационные системы и объекты, и, соответственно, имеют наибольший приоритет. Они, например, могут содержать:

- специальные требования к резервному копированию информации (такие как более высокая частота резервного копирования и использование более надежных носителей для этого);
- специальные требования к идентификации и аутентификации пользователей (такие как комбинирование биометрической идентификации и идентификации при помощи паролей);
- специальные требования к копировально-множительной технике, используемой для работы с конфиденциальной информацией;
- специальные требования к помещениям, в которых проводятся совещания по секретной тематике, и обрабатывается соответствующая информация (толщина и материал стен, расположение помещений в зданиях, защищенность окон, надежность дверей и запоров, а также охранной и пожарной сигнализации, обследования на предмет выявления подслушивающих устройств и пр.).

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)

К политикам второго типа могут относиться:

- политика опубликования открытых информационных материалов, в том числе политика организации веб-сайта предприятия и его внутреннего информационного портала (в части предотвращения возможных утечек и искажений информации);
- политика использования сети Интернет (в части предотвращения возможных утечек информации);
- политики использования отдельных информационных и коммуникационных технологий, в том числе общие для всего предприятия правила использования мобильных компьютеров и КПК, удаленного доступа к корпоративным информационным системам, а также использования личных компьютеров сотрудников предприятия в служебных целях;
- классификации информационных систем, информационных ресурсов и объектов информации с точки зрения их значимости и усилий, которые необходимо предпринимать для их защиты;
- политика приобретения, установки, модификации и обновления программного обеспечения, а также аутсорсинга разработки и проектирования программного обеспечения;
- политика закупки аппаратных средств информационных систем, систем информационной безопасности;
- политика использования пользователями собственного программного обеспечения (т.е. ПО, самостоятельно разрабатываемого предприятием);
- общие для всего предприятия правила использования паролей и других средств персональной идентификации;
- политика использования электронно-цифровой подписи и инфраструктуры публичных ключей;
- политика (регламент) обеспечения внутриобъектового режима и физической защищенности информационных активов;

- политика доступа к внутренним информационным ресурсам сторонних пользователей (организаций);
- общий для всего предприятия порядок привлечения к ответственности за нарушение определенных правил информационной безопасности.

3.4 Политика информационной безопасности предприятия – нижний уровень

Данный уровень включает в себя документы, являющиеся инструкциями и методиками прямого действия, используемыми в повседневной деятельности сотрудников предприятия. Эти документы относятся к отдельным сервисам, процедурам и информационным системам. Основной задачей разработки организационной документации на этом уровне является обеспечение как можно более детального и формализованного описания всех процедур и требований, относящихся к обеспечению безопасности отдельных элементов информационных систем, информационных потоков и массивов информации. В частности, для обеспечения полноты формирования политики информационной безопасности предприятия необходимо сформировать как можно более полный комплект организационной документации, включающий в себя:

- бланки типовых заявок на предоставление доступа отдельных сотрудников к определенным информационным ресурсам и информационным системам, а также регламенты предоставления такого доступа;
- регламенты (процедуры) работы с определенными информационными и телекоммуникационными системами, программным обеспечением и базами данных;
- должностные обязанности отдельных категорий сотрудников в отношении обеспечения информационной безопасности, а также требования, предъявляемые к персоналу;
- типовые договоры с внешними контрагентами, связанные с передачей или получением информации, или основные требования, предъявляемые к таким договорам.

Процедурные документы, относящиеся к предоставлению доступа к ресурсам (таким как сеть Интернет, корпоративные информационные системы и базы данных, аппаратные средства, средства передачи информации и пр.) могут включать как типовые бланки заявок на предоставление доступа, так и описание основных процедур (регламента) принятия решений о предоставлении такого доступа и предоставлении конкретных прав при работе с информационными ресурсами, а также перечни критериев, необходимых для предоставления тех или иных прав в информационных системах.

Процедуры работы с отдельными информационными системами и/или модулями информационных систем (базами данных, модулями корпоративной ERP-системы, системами электронного документооборота и пр.) могут перечислять все основные требования, правила и ограничения, например, запрет, использовать дискеты для копирования и переноса информации или ограничения, налагаемые на возможность удаленного доступа к тем или иным информационным сервисам. Требования и правила, связанные с обеспечением информационной безопасности, могут быть, как включены в общие инструкции по использованию информационных систем или регламенты осуществления бизнес-процессов, так и оформлены в виде специальных инструкций и памяток, содержащих исключительно требования и правила информационной безопасности.

Должностные обязанности персонала предприятия, связанные с обеспечением информационной безопасности, должны входить как составная часть в должностные инструкции для каждого сотрудника. Кроме того, политика безопасности может предусматривать подписание (как при поступлении на работу или переводе на определенную должность, так и при увольнении с нее) отдельными категориями персонала дополнительных соглашений, обязательств и подписок о неразглашении определенной информации. Также политика безопасности может вводить дополнительные требования к персоналу, работающему с определенными сведениями или информационными системами. Примерами таких ограничений могут быть отсутствие судимости, наличие

определенных навыков или специальной квалификации, прохождение профессиональной сертификации или психологической проверки.

Политики безопасности, относящиеся к работе с внешними контрагентами, могут предусматривать типовые формы и отдельные инструкции по составлению коммерческих контрактов (для каждого типа контрактов, а также для отдельных групп контрагентов) и обмену информацией с поставщиками, покупателями, консультантами, посредниками, субподрядчиками, поставщиками финансовых и информационных услуг и другими участниками хозяйственной деятельности. В частности, в политике для каждой из этих категорий может предусматриваться специфический порядок информационного обмена, взаимные требования по обеспечению конфиденциальности и возможные меры ответственности в случае нарушения согласованных требований какой-либо из сторон.

3.5 Заключительные положения

В тех случаях, когда определенная политика безопасности описывает сложную информационную систему и систему защиты информации, предназначенную для выполнения наиболее ответственных операций (таких как, например, электронные денежные переводы), она может быть разделена на две составляющие:

- внутренний регламент работы подразделений (групп, администраторов), отвечающих за выполнение наиболее важных административных функций (например, выдача и обслуживание электронных сертификатов Инфраструктуры публичных ключей);
- политику, непосредственно отражающую требования к пользователям и процессам, а также описания процедур работы и взаимодействия всех участников информационного обмена.

В этом случае внутренний регламент может содержать подробное описание тех правил и требований, которые должны выполнять ответственные подразделения (ИТ-служба, Департамент информационной безопасности или

Служба безопасности предприятия) в процессе выполнения своих функций. Такой регламент может быть необходим для демонстрации надежности наиболее важных и ответственных элементов инфраструктуры информационной безопасности. Это особенно важно в том случае, если предприятие осуществляет информационный обмен с внешними контрагентами (и, в частности, клиентами) и демонстрация надежности внутренних процедур сервисов информационной безопасности может обеспечить расширение бизнеса и повышение эффективности отдельных операций.

В некоторых случаях объем таких документов (политик, регламентов) может достигать нескольких десятков страниц (как правило, не более 100-150 страниц). Документы такого размера, как правило, составляются в тех случаях, когда может понадобиться их использование в судебных процессах для установления степени вины и ответственности различных участников процедур информационного обмена. В том случае, если отдельные политики представляют собой сложные объемные документы, изобилующие юридическими и техническими терминами, они могут сопровождаться дополнительным документом, кратко раскрывающим основные требования и положения для большинства пользователей. Такой документ должен иметь относительно небольшой объем (например, не более двух страниц) и содержать описание наиболее важных аспектов предмета политики: практически важные ограничения, ответственность и основные правила, знание которых необходимо для повседневной деятельности.

К числу документов на среднем и нижнем уровне детализации, помимо собственно политик безопасности, можно отнести также юридическое заключение, формально подтверждающее, что все меры информационной безопасности, предпринимаемые на предприятии, соответствуют требованиям действующего законодательства и/или стандартов.

1 Внутриобъектовый режим; охрана помещений и территорий

Организация внутриобъектового режима и охраны помещений и территорий является частью общей работы предприятия по обеспечению сохранности имущества и непрерывности текущей деятельности. Основной задачей обеспечения внутриобъектового режима является недопущение посторонних лиц к информационным активам и предотвращение угроз информационной безопасности.

Основой внутриобъектового режима является пропускной режим, в рамках которого, как правило, устанавливаются:

- документы, дающие право прохода на территорию предприятия – как пропуска и карты доступа, выданные самим предприятием, так и документы, выданные сторонними организациями (например, служебные удостоверения должностных лиц некоторых органов государственной власти);
- категории пропусков, используемых на предприятии, в соответствии с которыми (категориями) ограничивается срок действия пропусков, время возможного прохода на территорию предприятия (дни недели, часы суток) и некоторые другие параметры;
- порядок выдачи, обмена, продления и изъятия пропусков, а также порядок действий сотрудников и должностных лиц при утрате пропуска;
- порядок организации пропуска лиц, автотранспорта и проноса (провоза) имущества: размещение и порядок работы контрольно-пропускных пунктов, возможность пропуска тех или иных лиц, средств автотранспорта и грузов через те или иные КПП и пр.;
- основные положения документооборота, используемого при проходе посетителей на территорию предприятия — требования к ведению Журнала регистрации прохода посетителей, требования к документам, на основе которых выдаются разовые пропуска, порядок выдачи разовых пропусков и пр.;
- порядок досмотра транспортных средств, допускаемых на территорию предприятия.

Кроме того, в рамках организации внутриобъектового режима может быть предусмотрено разделение помещений и территорий на отдельные зоны с ограничением доступа (в том числе на основе разделения помещений и территорий на различные категории), а также разграничение доступа отдельных сотрудников (категорий персонала) и посетителей в различные зоны; также могут быть определены основные требования к техническим средствам разграничения доступа и организации их использования.

С технической точки зрения меры по обеспечению пропускного и внутриобъектового режимов могут быть реализованы теми же средствами, которые используются для обеспечения безопасности в других сферах, помимо информационной (защита имущества и персонала, обеспечение непрерывности производственного процесса), – средствами контроля доступа, видеонаблюдения, сигнализации и физической защиты.

В основе средств контроля доступа лежат механизмы опознавания личности и сравнения с установленными параметрами. Политика предприятия может устанавливать как упрощенные подходы к опознаванию, когда охранники предприятия проверяют документы (подтверждение личности, подтверждение возможности прохода на территорию в данное время через данный КПП), так и использование автоматизированных средств, когда опознавание посетителя и подтверждение (либо запрет) возможности прохода на территорию (выхода с территории, из здания) производится автоматизированной системой контроля доступа на основе имеющихся у посетителя машиночитаемых средств персональной идентификации (пластиковых карт, жетонов и пр.) либо на основе считывания и анализа его физических особенностей (геометрии лица, отпечатков пальцев, рисунка радужной оболочки глаза, голоса и пр.). При выборе конкретных средств биометрической идентификации специалистам и руководителям предприятия следует помнить, что разные технологии имеют разную степень надежности, а также могут быть более или менее удобными в повседневном использовании большим количеством людей. Так, например, считается, что одна из передовых

технологий биометрической идентификации – идентификация по кровеносным сосудам пальца (когда инфракрасный луч просвечивает палец и создает трехмерное изображение уникальной для каждого человека структуры кровеносных сосудов) – существенно менее уязвима для обмана, чем дактилоскопическая идентификация.

Физическая защита объектов, как правило, предполагает усиление конструкций ограждений, элементов зданий, сооружений и отдельных помещений. К таким средствам относятся защита оконных проемов металлическими решетками и ставнями, специальное остекление окон, использование бронированных дверей, запирающих устройств, сейфов для хранения средств вычислительной техники и носителей информации. В соответствии с особенностями используемых помещений и территорий политика безопасности предприятия также может предусматривать расположение мест хранения и обработки информации (например, архивов или серверных комнат) в помещениях, наименее доступных для проникновения, наиболее удаленных от мест хранения взрывоопасных и легковоспламеняющихся веществ, наименее подверженных затоплению (для объектов расположенных в долинах рек и на побережье), наиболее защищенных от ударов молнии и пр.

С физической защитой непосредственно связано использование средств сигнализации и видеонаблюдения. В зависимости от характера охраняемого объекта (территория, здание, проход, помещение, отдельный шкаф или сейф) в средствах сигнализации могут применяться датчики, работающие на различных физических принципах (фотоэлектрические датчики, датчики объема, акустические датчики и пр.), имеющие различные настройки и использующие различные каналы связи. В отличие от средств сигнализации средства видеонаблюдения позволяют не только установить факт нарушения, но и в деталях отслеживать его, контролировать ситуацию, а также вести видеозапись, которую можно будет использовать для принятия дальнейших мер (поиск нарушителей, уголовное преследование и пр.).

Отдельной задачей является обеспечение информационной безопасности при процессе транспортировки носителей информации и других объектов, требующее использования как специальных организационных приемов, так и специальных технических средств. К организационным методам относится привлечение специально подготовленных курьеров, а также разделение носителей информации (объектов) на части и их раздельная транспортировка с целью минимизации возможностей утечки информации. К техническим средствам, применяемым при транспортировке объектов, относятся защищенные контейнеры, специальные упаковочные материалы, а также тонкопленочные материалы и голографические метки, позволяющие идентифицировать подлинность объектов и контролировать несанкционированный доступ к ним.

2 Физическая защита объектов

Физическая защита объектов, как правило, предполагает усиление конструкций ограждений, элементов зданий, сооружений и отдельных помещений. К таким средствам относятся защита оконных проемов металлическими решетками и ставнями, специальное остекление окон, использование бронированных дверей, запирающих устройств, сейфов для хранения средств вычислительной техники и носителей информации. В соответствии с особенностями используемых помещений и территорий политика безопасности предприятия также может предусматривать расположение мест хранения и обработки информации (например, архивов или серверных комнат) в помещениях, наименее доступных для проникновения, наиболее удаленных от мест хранения взрывоопасных и легковоспламеняющихся веществ, наименее подверженных затоплению (для объектов расположенных в долинах рек и на побережье), наиболее защищенных от ударов молнии и пр.

С физической защитой непосредственно связано использование средств сигнализации и видеонаблюдения. В зависимости от характера охраняемого объекта (территория, здание, проход, помещение, отдельный шкаф или сейф) в

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)

средствах сигнализации могут применяться датчики, работающие на различных физических принципах (фотоэлектрические датчики, датчики объема, акустические датчики и пр.), имеющие различные настройки и использующие различные каналы связи. В отличие от средств сигнализации средства видеонаблюдения позволяют не только установить факт нарушения, но и в деталях отслеживать его, контролировать ситуацию, а также вести видеозапись, которую можно будет использовать для принятия дальнейших мер (поиск нарушителей, уголовное преследование и пр.).

Отдельной задачей является обеспечение информационной безопасности при процессе транспортировки носителей информации и других объектов, требующее использования как специальных организационных приемов, так и специальных технических средств. К организационным методам относится привлечение специально подготовленных курьеров, а также разделение носителей информации (объектов) на части и их раздельная транспортировка с целью минимизации возможностей утечки информации. К техническим средствам, применяемым при транспортировке объектов, относятся защищенные контейнеры, специальные упаковочные материалы, а также тонкопленочные материалы и голографические метки, позволяющие идентифицировать подлинность объектов и контролировать несанкционированный доступ к ним.

3 Организация режима секретности

Организация режима секретности в учреждениях и на предприятиях в РФ основывается на требованиях федерального законодательства, касающегося вопросов государственной тайны, и соответствующих подзаконных актов. В соответствии с действующими нормами к государственной тайне может быть отнесена информация, касающаяся обороноспособности страны, ее экономики, международных отношений, государственной безопасности и охраны правопорядка (в том числе сведения о методах и средствах защиты секретной информации, а также о государственных программах и мероприятиях в области защиты государственной тайны); в законодательстве также специально уточняются области деятельности, информация о которых не может быть отнесена к государственной тайне. Отнесение конкретной информации к государственной тайне производится решением специально назначаемых должностных лиц, а общий Перечень сведений, отнесенных к государственной тайне, утверждается Президентом РФ и подлежит обязательному опубликованию. Для сведений, составляющих государственную тайну, устанавливаются три степени секретности: «особой важности», «совершенно секретно» и «секретно», а носители таких сведений (документы) должны иметь соответствующие реквизиты.

Основным элементом организации режима секретности является допуск должностных лиц и граждан к сведениям, составляющим государственную тайну. Он предполагает выполнение руководством предприятия и подразделений по защите государственной тайны (во взаимодействии с уполномоченными правоохранительными органами) следующих основных мероприятий:

- 1) Ознакомление должностных лиц и граждан с нормами законодательства, предусматривающими ответственность за нарушение требований.

- 2) Получение согласия на временные ограничения их прав в соответствии с законодательством.

3) Получение согласия на проведение в отношении их проверочных мероприятий.

4) Принятие решения о допуске к сведениям, составляющим государственную тайну.

5) Заключение с лицами, получившими допуск, трудового договора (контракта), отражающего взаимные обязательства таких лиц и администрации предприятия (в т.ч. обязательства таких лиц перед государством по нераспространению доверенных им сведений, составляющих государственную тайну).

Помимо отнесения сведений к государственной тайне и допуска должностных лиц и граждан к засекреченным сведениям, важным элементом системы обеспечения режима секретности является организация информационного обмена между предприятиями при совместном выполнении работ. В частности, передача засекреченных сведений от одного предприятия к другому должна производиться с разрешения уполномоченного государственного органа, договор на выполнение работ должен предусматривать обязательства сторон по обеспечению сохранности сведений, а заказчик работ должен контролировать выполнение нормативных требований контрагентами по таким договорам (наличие лицензий, оформление допуска сотрудников и пр.) и принимать необходимые меры в случае выявления нарушений.

Также важным элементом обеспечения режима секретности является организация передачи сведений, составляющих государственную тайну, другим государствам (в том числе ознакомление с такими сведениями и предоставление возможности доступа к ним). В каждом отдельном случае решение о передаче сведений выносится Правительством РФ на основании экспертного заключения Межведомственной комиссии по защите государственной тайны, которая, в свою очередь, руководствуется мотивированным ходатайством предприятия, заинтересованного в передаче секретных сведений, и решением органа государственной власти, курирующего

круг вопросов, к которому относятся передаваемые сведения. Для обеспечения защиты интересов РФ со стороны, принимающей секретные сведения, заключается договор, содержащий необходимые обязательства по защите получаемой информации, а также порядок разрешения конфликтных ситуаций и компенсации возможного ущерба.

4 Характеристики политик безопасности

4.1 Политика опубликования материалов в открытых источниках

Политика опубликования материалов в открытых источниках (таких как газеты, журналы, выставки, сеть Интернет, радио- и телепередачи, конференции, музейные экспозиции и пр.) должна обеспечивать предотвращение случайных и организованных утечек конфиденциальной информации при взаимодействии предприятия со средствами массовой информации, общественными и государственными органами, научным, академическим и бизнес-сообществом. Для того чтобы избежать ущерба интересам предприятия, такая политика должна содержать основные правила и процедуры подготовки информационных материалов к открытому опубликованию.

В частности, в политике безопасности следует предусматривать создание специального экспертного совета, ответственного за рассмотрение всех информационных материалов, которые предполагается опубликовать в открытых источниках (политика безопасности должна содержать конкретные ограничения на опубликование информационных материалов без их рассмотрения экспертным советом). Основной задачей такого совета является подготовка заключений о возможности или невозможности опубликования определенных информационных материалов, а также подготовка конкретных предложений по изъятию определенных сведений из материалов, подготавливаемых к опубликованию. При отсутствии единого мнения у членов экспертной комиссии решение о возможности опубликования может быть принято руководителем предприятия с учетом рекомендаций экспертов. Для эффективного решения задач члены экспертного совета должны детально знать

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)

все существующие ограничения (в частности, установленные законодательством) и владеть ситуацией в той сфере, в которой функционирует предприятие. При этом, как правило, сам автор подготавливаемых к опубликованию материалов не может входить в экспертный совет, а редактор или руководитель, отвечающий за подготовку материалов, не может быть председателем экспертного совета.

Характерным примером политики использования сети Интернет являются некоторые положения Указа Президента РФ от 12 мая 2004 года № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена», регламентирующего вопросы подключения локальных сетей и персональных компьютеров к сети Интернет, а также размещение информации в сети Интернет для некоторых категорий пользователей. Данный документ:

- запрещает включение информационных систем, сетей связи и автономных персональных компьютеров, где обрабатывается информация, содержащая сведения, которые составляют государственную тайну, и служебная информация ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам, в состав средств международного информационного обмена, в том числе в сеть «Интернет»;

- предписывает владельцам открытых и общедоступных государственных информационных ресурсов осуществлять их включение в состав объектов международного информационного обмена только при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации.

4.2 Политика управления паролями

Политика управления паролями (или, в более общем виде, политика идентификации и аутентификации) может определять периодичность замены паролей, действия, которые необходимо осуществить при компрометации паролей, основные требования к их качеству, процедурам их генерации, распределению основных обязанностей, связанных с генерацией паролей, их сменой и доведением до пользователей, а также основные меры ответственности за нарушение установленных правил и требований. Политика на этом уровне также может устанавливать запрет хранения записанных паролей, запрет сообщать кому-либо свой пароль (в том числе руководителям и администраторам информационных систем) и другие аналогичные ограничения.

4.3 Политика установки и обновления версий программного обеспечения

Политика установки и обновления версий программного обеспечения может включать в себя некоторые ограничения на самостоятельное приобретение и установку программного обеспечения отдельными подразделениями и пользователями, а также определенные требования к квалификации специалистов, осуществляющих их установку, настройку и поддержку.

4.4 Политика приобретения информационных систем и их элементов

Политика приобретения информационных систем и их элементов (программных и аппаратных средств) может включать в себя требования к лицензированию и сертификации используемых программного обеспечения и оборудования, а также определенные требования к фирмам, осуществляющим их поставку и внедрение.

4.5 Политика доступа сторонних пользователей (организаций)

Политика доступа сторонних пользователей (организаций) в информационные системы предприятия может содержать перечень основных ситуаций, когда такой доступ возможен, а также основные критерии и процедуры, в соответствии с которыми осуществляется доступ. Также политика может предусматривать распределение ответственности сотрудников самого предприятия за действия внешних пользователей, которые получают такой доступ.

4.6 Политика в отношении разработки ПО

Политика в отношении разработки ПО может содержать требования как к вопросам безопасности и надежности программных средств, самостоятельно разрабатываемых предприятием, так и в отношении передачи разработки программных средств (модулей информационных систем, отдельных программных библиотек и пр.) сторонним специализированным организациям (т.н. «аутсорсинг»), а также в отношении приобретения и использования тиражируемых программных библиотек (модулей), распространяемых компаниями-производителями. В частности, политика может содержать требования к тестированию самостоятельно разрабатываемого ПО, анализу его исходных кодов, описывать основные критерии надежности и пр.

4.7 Политики использования отдельных универсальных информационных технологий

Политики использования отдельных универсальных информационных технологий в масштабе всего предприятия могут включать в себя:

- политику использования электронной почты (e-mail);
- политику использования средств шифрования данных;
- политику защиты от компьютерных вирусов и других вредоносных программ;
- политику использования модемов и других аналогичных коммуникационных средств;

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)

- политику использования Инфраструктуры публичных ключей;
- политику использования технологии Виртуальных частных сетей (Virtual Private Network – VPN).

Политика использования электронной почты может включать в себя как общие ограничения на ее использование определенными категориями сотрудников, так и требования к управлению доступом и сохранению конфиденциальности сообщений, а также к администрированию почтовой системы и хранению электронных сообщений. Кроме того, политика может предусматривать:

- запрет на использование электронной почты в личных целях;
- специальные требования к отправке и получению присоединенных файлов, которые потенциально могут содержать вредоносные программы;
- запрет на использование электронной почты временными сотрудниками;
- требования шифрования передаваемых сообщений;
- наблюдение за всеми передаваемыми и получаемыми сообщениями;
- ограничения на передачу конфиденциальной информации при помощи электронной почты и другие положения.

4.8 Политика использования коммуникационных средств

Политика использования коммуникационных средств может определять границы использования технологий, позволяющих подключить компьютеры и информационные системы предприятия к информационным системам и коммуникационным каналам за его пределами. В частности, такая политика может вводить определенные ограничения на использование модемов для телефонных линий, устройств, использующих современные беспроводные технологии, такие, как GSM (GPRS), Wi-Fi, передача данных в сетях стандарта CDMA и пр.

4.9 Политика использования мобильных аппаратных средств

Политика использования мобильных аппаратных средств может относиться к различным устройствам, таким как мобильные ПК, КПК (PDA), переносные устройства хранения информации (дискеты, USB-flash, карты памяти, подключаемые жесткие диски и пр.). Она может отражать общее отношение предприятия к использованию сотрудниками таких устройств, определять требования и устанавливать конкретные области, в которых их использование допустимо. Также могут устанавливаться дополнительные общие требования к стационарному оборудованию в целях ограничения подключения к ним мобильных компьютеров и средств переноса данных.

1 Департамент информационной безопасности

Департамент информационной безопасности (далее – департамент) предприятия представляет собой самостоятельное структурное подразделение предприятия, непосредственно выполняющее ключевые функции защиты информационных ресурсов.

Его основными задачами, как правило, являются:

- организация и координация работ по обеспечению комплексной защиты информации на предприятии;
- контроль за выполнением установленных требований, и оценка эффективности работы подразделений и персонала предприятия по обеспечению информационной безопасности;
- выполнение отдельных административных и технических функций по обеспечению информационной безопасности, в т.ч.:
 - а) формирование, поддержка и документальное обеспечение политики информационной безопасности на всех уровнях;
 - б) внедрение различных средств защиты информации;
 - в) администрирование отдельных информационных систем.

Состав задач департамента, и его внутренняя организационная структура в каждом конкретном случае определяется такими особенностями функционирования предприятия, как:

- значимость информационных ресурсов в работе предприятия и характер существующих угроз;
- отношение руководства и собственников предприятия к вопросам информационной безопасности и их управленческая квалификация;
- функциональность и характер используемых информационных систем, их роль в бизнес-процессах;
- организация работы и структура ИТ-службы;
- финансовое состояние предприятия.

Таким образом, решение о составе и структуре департамента в каждом случае должно быть индивидуальным и учитывающим все основные условия.

1) Функции, связанные с формированием, поддержкой и документальным обеспечением политики информационной безопасности предприятия, могут включать в себя:

- консультирование руководителей и собственников предприятия по вопросам разработки и совершенствования политики информационной безопасности;

- самостоятельная разработка политики безопасности, ее согласование и представление ее руководству предприятия для утверждения, а также внесение необходимых изменений по мере изменения условий работы предприятия;

- самостоятельная разработка политик безопасности, касающихся отдельных вопросов защиты информации (правил применения телекоммуникационных технологий, требований, обязательных для всех используемых на предприятии персональных компьютеров и пр.);

- формирование требований и регламента процедур пересмотра политики безопасности, отдельных правил, типовых форм и других документов;

- анализ отдельных договоров и соглашений со сторонними организациями (поставщиками, покупателями, партнерами по проведению НИОКР и пр.) на предмет соответствия требованиям политики информационной безопасности;

- анализ и обобщение передового опыта и современных теорий в сфере управления информационной безопасностью с целью их практического применения на предприятии;

- привлечение сторонних специалистов, исследователей, консультантов (консалтинговых компаний) для разработки и совершенствования политики

безопасности предприятия и внедрения развитых методов управления в этой сфере;

- управление обучением персонала компании (контроль за полнотой и правильностью материалов учебных программ, связанных с информационной безопасностью, обеспечение своевременности прохождения обучения и пр.);

- консультирование специалистов и руководителей подразделений предприятия по вопросам соответствия разрабатываемых внутренних документов отдельных подразделений требованиям политики безопасности предприятия;

- контроль соответствия внутренних организационных документов предприятия (правил внутреннего распорядка, должностных инструкций, инструкций по использованию информационных систем, типовых форм договоров и пр.) требованиям политики информационной безопасности, а также согласование таких документов при их утверждении.

2) Функции, связанные с внедрением средств защиты информации, могут включать в себя:

- анализ современных программных и аппаратных средств защиты информации и связанных с ними методик защиты, а также рынка доступных средств защиты информации, применяемых для различных целей, и подготовка обоснованных предложений по приобретению определенных продуктов у определенных поставщиков;

- анализ закупаемых информационных систем (операционных систем, прикладных программ, телекоммуникационного оборудования, вычислительной техники и пр.) на предмет их потенциальной надежности и наличия уязвимостей;

- привлечение сторонних экспертов и консультантов для анализа закупаемых и используемых средств защиты информации с точки зрения их надежности, а также с точки зрения целесообразности их применения (внедрения);

Тема 2.5 – Департамент информационной безопасности и работа с персоналом
(Планирование и управление информационной безопасностью)

- формулирование требований (связанных с обеспечением информационной безопасности) к самостоятельно разрабатываемым программным продуктам или программному обеспечению, создаваемому на заказ сторонними разработчиками;
- участие в проектировании новых информационных систем, а также тестировании вновь разработанных и внедряемых программных продуктов;
- разработку технико-экономического обоснования для проектов внедрения средств защиты информации, а также привлечение для этих целей сторонних аналитиков и консультантов, специализирующихся на вопросах анализа средств защиты информации;
- подготовку обоснованных решений о выборе между самостоятельной разработкой средств защиты информации (например, программных модулей, осуществляющих шифрование данных) и передачей их разработки сторонним компаниям.

3) Функции, связанные с администрированием информационных систем и систем защиты информации, могут включать в себя:

- выполнение некоторых функций по администрированию отдельных информационных систем (баз данных, систем коллективной работы с документами, почтовых систем и пр.), а также администрирование и конфигурирование систем защиты информации (межсетевых экранов, систем обнаружения вторжений и пр.);
- определение требуемых типовых настроек и конфигураций рабочих станций (персональных компьютеров), имеющих отношение к информационным системам предприятия (в частности, подключенных к его локальной сети);
- привлечение сторонних организаций для осуществления текущего администрирования информационных систем и систем защиты информации, а также для консультационной и технической поддержки при возникновении

Тема 2.5 – Департамент информационной безопасности и работа с персоналом
(Планирование и управление информационной безопасностью)

инцидентов, связанных с информационной безопасностью (в частности, при осуществлении нападений на информационные системы предприятия);

- установку (в том числе и совместно со специалистами ИТ-подразделения) программных и аппаратных средств защиты информации на рабочие места пользователей и в другие элементы информационных систем;

- консультирование пользователей по возникающим вопросам, связанным с информационной безопасностью, и оперативное разрешение возникающих у них проблем;

- реагирование на различные инциденты, связанные с нарушением информационной безопасности;

- принятие активных встречных мер при обнаружении вторжений в информационную систему (информирование правоохранительных органов, самостоятельный поиск нападающих и пр.);

- генерирование паролей пользователей информационных систем и обеспечение их сохранности;

- участие в восстановлении работоспособности информационных систем после сбоев и нарушений в работе.

4) Функции, связанные с контролем выполнения требований политики информационной безопасности и проведением аудитов могут включать в себя:

- сбор и анализ сведений о нарушениях различных требований политики безопасности, поступающих из различных источников (в том числе и от администраторов информационных систем) и определение приоритетных направлений контрольной работы;

- проверку организационной документации отдельных подразделений предприятия на предмет соответствия требованиям политики информационной безопасности (в том числе и своевременности внесения всех необходимых изменений в действующие внутренние организационные документы);

- проверку состояния (правильности ведения) текущей хозяйственной и кадровой документации отдельных подразделений предприятия, связанной с

обеспечением информационной безопасности (правильности и своевременности заполнения журналов, своевременность оформления обязательств о неразглашении сведений сотрудниками и пр.);

- проведение комплексных аудитов информационной безопасности на предприятии;

- организацию контрольных проверок защищенности отдельных элементов информационных систем (серверов, сегментов сети и пр.);

- привлечение сторонних организаций для проведения аудитов информационной безопасности на предприятии, проверок надежности информационных систем.

5) Кроме перечисленных функций, непосредственно связанных с защитой информационных ресурсов, также большое значение имеет выполнение функций, связанных с охраной имущества предприятия и решением задач, которые связаны с обеспечением безопасности предприятия в более широком смысле. В частности, для обеспечения информационной безопасности имеет значение выполнение таких функций, как:

- охрана территории и имущества предприятия, а также охрана персонала;

- обеспечение соблюдения пропускного режима;

- наблюдение за территорией и помещениями (в том числе при помощи видеокамер);

- контроль за ввозом на территорию предприятия и вывозом готовой продукции, материалов, документов и другого имущества;

- организация внутренних служебных проверок и расследований, а также взаимодействия с правоохранительными органами;

- контроль за соблюдением временного режима работы, а также за соблюдением правил внутреннего распорядка.

2 Организационная структура и персонал департамента информационной безопасности

На практике департамент является подразделением, либо напрямую подчиняющимся первому лицу предприятия, либо входящим в качестве структурной единицы в службу безопасности предприятия. Сотрудники департамента находятся в административном и функциональном подчинении у руководителя департамента¹, который несет ответственность за обеспечение информационной безопасности на предприятии. Вывод департаментов информационной безопасности из структуры ИТ-служб на предприятиях является одной из важных современных тенденций в управлении бизнесом, информационными технологиями и информационной безопасностью, т.к., по мнению некоторых специалистов, у этих подразделений имеются некоторые частично взаимопротиворечащие интересы и потому некоторые задачи не могут быть эффективно решены в рамках одного структурного подразделения.

В составе департамента для повышения эффективности работы могут быть выделены самостоятельные группы (отделы), специализирующиеся на выполнении определенных функций (Рисунок 1):

- отдел (группа, бюро) нормативной (организационной) документации;
- отдел (группа, бюро) администрирования информационных систем;
- отдел (группа, бюро) аудита информационной безопасности;
- отдел (группа, бюро) внедрения информационных систем и систем защиты информации.

Отдел нормативной документации решает задачи, связанные с формированием, поддержкой и документальным обеспечением политики информационной безопасности предприятия, и должен, главным образом, включать в себя специалистов по менеджменту и бизнес-анализу, прошедших дополнительную подготовку в сфере управления информационной безопасностью.



Рисунок 1 – Структура департамента ИБ

Также в состав такого отдела могут входить юристы. Аналогичный кадровый состав может быть и у Отдела внутреннего аудита информационной безопасности. При этом к квалификации сотрудников Отдела нормативной документации, как правило, должны предъявляться гораздо более высокие профессиональные требования.

Отдел администрирования информационных систем, а также Отдел внедрения информационных систем и систем защиты информации, как правило, должны включать в себя специалистов по информационным технологиям и средствам защиты информации, имеющих значительный опыт внедрения и эксплуатации корпоративных информационных систем.

3 Работа с персоналом предприятия

Практическая реализация всех положений сформированной политики информационной безопасности потребует от предприятия длительных практических усилий. Одним из основных и наиболее сложных направлений работы является работа с персоналом, цели которой:

- отбор и предварительная проверка персонала, принимаемого на работу (на службу);
- обучение сотрудников;
- достижение взаимопонимания руководителей и сотрудников в вопросах обеспечения информационной безопасности;
- психологическая подготовка с целью противостояния методам т.н. «социальной инженерии».

В одной из своих книг известный специалист по проблемам информационной безопасности Брюс Шнайер заметил, что в общей системе мер по защите информации «математический аппарат является безупречным, компьютеры же уязвимы, сети вообще паршивы, а люди просто отвратительны. Я изучил множество вопросов, связанных с обеспечением безопасности компьютеров и сетей, и могу утверждать, что не существует решения проблемы человеческого фактора». Это высказывание наиболее ярко и наглядно демонстрирует важность целенаправленных мероприятий по подбору, расстановке и работе с кадрами предприятия с той целью, чтобы в работе информационных систем не возникло «узких мест» и т.н. человеческий фактор не стал наиболее весомым источником угроз для информационной безопасности. Основной причиной, определяющей значимость человеческого фактора в общей системе защиты информации, является то, что при всей развитости современных средств автоматизации информационные системы по-прежнему представляют собой человеко-машинные комплексы и их (систем) функционирование во многом зависит от работы отдельных людей. Именно по этой причине неадекватное обращение служащих предприятия с компонентами

информационной системы может нанести серьезный ущерб информационной безопасности даже при наличии детально проработанных политик безопасности и высокоэффективных программных и аппаратных средств защиты информации.

Начальная стадия работы – подбор и расстановка кадров – может иметь несколько аспектов. В первую очередь, основным критерием для назначения на определенные должности, связанные с работой со сведениями, которые составляют государственную тайну, является получение соответствующей формы допуска (эта процедура описана в предыдущем подразделе). В соответствии с требованиями действующих нормативно-правовых актов Перечень должностей, при назначении на которые необходимо оформлять специальный допуск, устанавливается руководителем предприятия и может периодически пересматриваться (для сведений, составляющих государственную тайну, не реже одного раза в 5 лет). Это требование связано, с одной стороны, с тем, что руководитель предприятия несет ответственность за обеспечение режима секретности, а с другой – с тем, что для выполнения функциональных обязанностей сотрудникам предприятия необходимо работать с определенными сведениями и, соответственно, иметь определенный уровень допуска.

Также при подборе и расстановке кадров могут применяться и менее формализованные методы. Это могут быть различные методики психологической оценки, включающие в себя:

- анализ мотивационных аспектов личности;
- оценку психологической устойчивости личности;
- оценку уровня познавательных способностей личности (успешность приобретения новых знаний и навыков и способность к их практическому применению);

– оценку активности личности в достижении поставленной цели, умение объективно оценивать ситуацию и людей, умение вырабатывать оптимальную стратегию поведения.

Такого рода анализ может быть необходим как в отношении специалистов и руководителей, которые работают с информацией, подлежащей защите, в связи с выполнением своих должностных обязанностей по основному профилю работы предприятия, так и специалистов, и руководителей, чьей основной задачей является обеспечение информационной безопасности предприятия (аудиторов ИБ, проектировщиков и администраторов информационных систем и систем защиты информации и пр.).

Помимо тщательного подбора, одной из важных основ работы с персоналом является его обучение способам обеспечения информационной безопасности и безопасной работе с информационными системами. Обучение и последующий контроль полученных (имеющихся) знаний может быть, как первичным, так и повторным. В общем случае сотрудник предприятия не может быть допущен к выполнению своих должностных обязанностей и работе с информационными системами до тех пор, пока он не пройдет обучение по вопросам информационной безопасности и не будет:

- детально ознакомлен со всеми действующими на предприятии требованиями и общими правилами;
- полностью обучен методам и приемам обеспечения информационной безопасности, необходимым для выполнения его должностных обязанностей;
- ознакомлен со всеми возможными мерами ответственности (дисциплинарной, административной, уголовной), которые могут быть к нему применены в случае нарушения требований, а также в случае нанесения ущерба по его вине.

В завершении всей предварительной работы сотрудник должен дать все необходимые обязательства о неразглашении конфиденциальных сведений, а также письменно засвидетельствовать, что он полностью ознакомлен с основными положениями политики безопасности. В процессе работы

предприятие также может проводить периодический контроль знаний и навыков, связанных с обеспечением информационной безопасности с той целью, чтобы засвидетельствовать компетентность работников в этой сфере. Также одним из инструментов обучения может быть периодическое ознакомление персонала с реальными примерами недавно произошедших инцидентов, связанных с информационной безопасностью. Кроме того, дополнительное обучение персонала предприятия может производиться в случаях:

- внедрения новых автоматизированных информационных систем;
- изменения бизнес-процессов предприятия;
- изменения требований политик безопасности (например, в связи с изменением требований законодательства).

Необходимость дополнительного обучения при внедрении новых информационных систем и, в частности, интегрированных систем управления предприятием, как правило, может быть обусловлена появлением новых функциональных возможностей программного обеспечения и изменением процедур обработки информации. Также доступ к интегрированным информационным системам потенциально может дать доступ к ранее недоступной информации и предоставить ранее отсутствовавшие возможности влиять на различные информационные потоки. В связи с этим может возникнуть потребность в том, чтобы сотрудники дали дополнительные обязательства о соблюдении мер информационной безопасности. Аналогичные организационные меры по обеспечению защиты информации могут быть необходимы и при изменении бизнес-процессов предприятия, когда меняется его структура, распределение функций между подразделениями и обязанностей сотрудников, и соответственно, вносятся изменения в организационные схемы, штатные расписания и должностные инструкции персонала. Изменения требований политики безопасности могут быть связаны с появлением новых угроз, изменением законодательных требований, расширением рынков,

изменением отношения руководства и собственников предприятия к вопросам информационной безопасности и другими факторами, – все эти уточнения и изменения также должны своевременно и в полном объеме доводиться до персонала.

В процессе обучения определенную значимость может иметь разъяснение рациональных причин, по которым предприятие применяет именно такую политику безопасности. Это может служить как для лучшего понимания и усвоения положений политики безопасности, так и для определенной разрядки психологической напряженности, неизбежно возникающей при принятии ограничительных мер и возложении дополнительных обязанностей, необходимость которых не всегда очевидна и понятна как рядовым сотрудникам, так и специалистам.

Отдельным направлением обучения и повышения квалификации может быть развитие у персонала компании навыков противодействия методам т.н. социальной инженерии (данный подход также иногда называют «социотехникой»). Использование для незаконного проникновения в информационные системы методов социальной инженерии связано с т.н. «человеческим фактором», который представляет собой совокупность определенных психологических склонностей и особенностей мышления и поведения, которые свойственны практически всем людям. К числу таких склонностей и особенностей можно отнести:

- неспособность адекватно оценить опасность в некоторых ситуациях;
- специфическое отношение к редко происходящим событиям (притупление внимания);
- излишнее доверие и полагание на средства автоматизации;
- подверженность манипулированию, основанная, например, на желании помочь людям (в том числе и незнакомым) или на излишнем доверии людям, одетым в специальную униформу, и пр.

Именно с использованием некоторых психологических особенностей такого рода осуществляются многие наиболее успешные (для нападающих) проникновения в корпоративные информационные системы. Примерами таких проникновений являются ситуации, когда злоумышленник:

- совершает телефонный звонок, представляется администратором и, сославшись на определенные обстоятельства (такие как сбой в системе), просит сообщить ему пароль;
- приходит в офис в специальной униформе (например, в форме сотрудника компании, занимающейся обслуживанием и ремонтом компьютеров) и просит предоставить ему доступ к информационной системе;
- присылает сообщение по электронной почте от имени администратора информационной системы или руководства предприятия и просит сообщить пароль или совершить определенные действия.

Большую значимость в общей системе мер по преодолению влияния человеческого фактора имеет повседневная работа с персоналом. Помимо обучения персонала и применения дисциплинарных мер воздействия, одной из основных задач такой работы является постоянное напоминание всем сотрудникам о необходимости соблюдения правил информационной безопасности. Конкретные способы, при помощи которых такие напоминания могут быть сделаны, будут зависеть от предпочтений руководителей предприятия, сложившейся корпоративной культуры, специфики бизнес-процессов и других обстоятельств. Характерными способами того, как предприятие может постоянно напоминать своим сотрудникам о необходимости соблюдать осторожность, являются:

- размещение и периодическая смена (обновление дизайна и содержания) напоминаний о необходимости соблюдать требования политики информационной безопасности на предметах, постоянно находящихся в поле зрения сотрудников в течение рабочего дня: настенных и настольных

Тема 2.5 – Департамент информационной безопасности и работа с персоналом
(Планирование и управление информационной безопасностью)

календарях, кофейных кружках, обложках блокнотов, настольных экспонатах, ручках, карандашах и других канцелярских принадлежностях;

- периодическая рассылка соответствующих брошюр, бюллетеней и буклетов, а также сообщений по электронной почте;

- использование скринсэйверов, содержащих соответствующие напоминания;

- использование голосовой почты и громкой связи для периодической передачи сообщений о необходимости соблюдения правил информационной безопасности и пр.

Таким образом, комплекс всех организационных мер по работе с персоналом предприятия, включающий в себя систему обучения персонала, систему привлечения нарушителей к ответственности, и постоянное поддержание атмосферы ответственного отношения к вопросам безопасности, должен в определенной мере уменьшить негативное влияние человеческого фактора на защищенность информационных систем и состояние информационной безопасности.

1 Организация реагирования на чрезвычайные ситуации (инциденты)

Реагирование на возникающие чрезвычайные ситуации (инциденты), связанные с нарушением информационной безопасности, является таким же важным направлением работы, как и построение системы защиты и предотвращения нарушений. Под инцидентом, как правило, понимается какое-либо отклонение от нормального процесса использования информационных ресурсов и функционирования информационных систем, повлекшее ущерб для определенных информационных активов предприятия или непосредственно создающее угрозу нанесения такого ущерба.

Чрезвычайная ситуация (инцидент), связанная с нарушением информационной безопасности, может быть обусловлена:

- разрушительным воздействием на весь имущественный комплекс предприятия при возникновении стихийных факторов (наводнение, пожар, землетрясение и пр.) или целенаправленном нападении (подрыв, поджог, разрушение зданий и помещений и пр.);
- негативным воздействием исключительно на информационные ресурсы предприятия (как правило, осуществляемым удаленно, с использованием телекоммуникационных каналов).

В общем случае организационные процедуры (регламенты) реагирования на чрезвычайные ситуации должны включать в себя:

- регламенты альтернативных процессов обработки информации (в том числе, возможно, и без использования средств автоматизации) на период выхода из строя основных информационных ресурсов;
- определение групп персонала, ответственных за выполнение тех или иных функций в случае возникновения чрезвычайной ситуации, а также определение процедур взаимодействия между группами и отдельных групп с руководством предприятия;

- техническую и организационную документацию, необходимую для восстановления информационных систем и данных после чрезвычайной ситуации;
- порядок хранения архивных (резервных) копий данных и программных приложений обработки данных в местах, защищенных от механических воздействий, краж, наводнений, пожаров и пр. (в т.ч., возможно, в местах, территориально удаленных от основных мест хранения и обработки информации);
- соглашения с поставщиками программных и аппаратных средств, входящих в информационную инфраструктуру предприятия, о срочной поставке компонент, вышедших из строя и требующих замены в случае чрезвычайной ситуации.

Процесс реагирования на такого рода инциденты включает в себя четыре основных этапа:

- 1) Обнаружение нападения.
- 2) Локализация нападения.
- 3) Идентификация нападающих;
- 4) Оценка и последующий анализ процесса нападения и его обстоятельств.

2 Обнаружение атак и распознавание вторжений

Обнаружение атак и распознавание вторжений, как правило, является инженерно-технической задачей, решаемой при помощи специальных программных и иногда аппаратных средств. В частности, обнаружение может осуществляться на основе анализа сетевого трафика и журналов (лог-файлов), в которых фиксируются различные действия. Обнаружение может осуществляться на основе т.н. сигнатур – формализованных наборов признаков определенных вирусов, типов атак и пр. Также, очевидно, источником информации о нарушениях являются сообщения пользователей об отклонениях

в работе информационных систем и появление явных негативных последствий произошедших нарушений.

Для обеспечения своевременного обнаружения нарушений предприятие должно организовать постоянную (при необходимости – круглосуточную) работу специалистов, отвечающих за разрешение инцидентов. Для этого может быть выбран один из возможных подходов.

1) Организация собственной дежурной службы, состоящей из компетентных специалистов, несущих посменное дежурство и оснащенных средствами мобильной связи.

2) Привлечение сторонней организации, специализирующейся на оказании подобных услуг.

При этом сотрудники предприятия должны знать номера телефонов и иные способы связи, при помощи которых они могли бы оперативно сообщать дежурным специалистам обо всех происшествиях. Важность организации как можно более оперативного информирования специалистов по безопасности и, соответственно, как можно более оперативного реагирования обусловлена тем, что обнаружение нападения и начало противодействия в то время, как само нападение еще продолжается, в большинстве случаев может быть гораздо более эффективным, чем реагирование после окончания нападения.

Выявление нарушений может быть осуществлено не только по явным признакам, таким как сообщения пользователей о прекращении функционирования отдельных элементов информационных систем, одновременное использование одной учетной записи на нескольких рабочих станциях или явное обнаружение вирусов в данных, передаваемых по локальной сети, но и по некоторым косвенным признакам (аномальным явлениям), которые в отдельных случаях могут свидетельствовать (а могут и не свидетельствовать) о нарушениях. Примерами таких косвенных свидетельств могут быть:

– использование информационных систем и определенных учетных записей в нехарактерное время (рано утром, поздно вечером и пр.);

Тема 2.6 – Чрезвычайные ситуации (инциденты)
(Управление информационной безопасностью)

- резкое нехарактерное повышение нагрузки на информационные системы или их отдельные элементы (сегменты сети, хранилища данных и пр.);
- изменение характера поведения пользователей (например, последовательности определенных действий при использовании информационной системы) и пр.

Для более эффективного анализа таких косвенных признаков и интерпретации различных фактов специалистам по реагированию на инциденты может понадобиться анализ функциональности информационных систем и взаимодействие аналитиков департамента информационной безопасности с пользователями (изучение особенностей их работы). Также для автоматизации такого анализа могут быть использованы специальные программные средства, автоматически осуществляющие статистический анализ сетевого трафика и других элементов информационной инфраструктуры и сигнализирующие при обнаружении аномальной активности, для того чтобы администраторы могли провести дальнейший качественный анализ выявленных отклонений и при необходимости предпринять активные ответные действия. В целом, разработка и совершенствование таких средств анализа в составе комплексных систем обнаружения вторжений является одним из перспективных направлений развития средств защиты информации.

Таким образом, основной задачей на начальном этапе реагирования является определение характера нарушений и достоверное установление того, что выявленные аномальные события, действия и характеристики являются действительно нарушениями, а, например, не проявлением особенностей работы программного обеспечения.

Одним из важнейших организационных аспектов реагирования на инциденты (и, в частности, на отдельные сигналы о некоторых происшествиях) является то обстоятельство, что может происходить более или менее частое поступление ложных сигналов (ошибочных или специально спровоцированных) о некоторых происшествиях, и реакция персонала

департамента информационной безопасности со временем может постепенно ослабевать (так же как, например, может притупиться внимание при частых ложных срабатываниях охранной сигнализации). В частности, по оценке некоторых специалистов, в среднем в 90% случаев, когда пользователи сообщают о том, что, по их мнению, компьютер заражен вирусом, они ошибаются. В связи с этим при организации реагирования на инциденты необходимо уделить особое внимание психологической подготовке персонала, отвечающего за реагирование, а также по возможности анализировать причины появления таких ложных сигналов и предотвращать их в дальнейшем.

Также значимым вопросом организации работы с пользователями в ситуациях реагирования на инциденты является то, что взаимодействие между пользователями и группами реагирования, а также различных групп реагирования между собой по возможности необходимо осуществлять по специальным защищенным каналам связи.

3 Локализация и устранение последствий

Локализация и устранение последствий является основным этапом, в рамках которого, собственно, осуществляется реагирование на инцидент. На этом этапе происходит:

- определение конкретных параметров нарушения (нападения), его характера (конкретных сегментов сети, серверов, групп рабочих станций, приложений, затронутых нападением);
- предварительный анализ действий нарушителя и сценария произошедшего (происходящего) нападения, алгоритма работы появившегося вируса и пр.;
- блокирование действий нарушителя (если нарушение является длящимся);
- блокирование (полное или частичное) работы информационной системы (сервера, базы данных, сегмента сети и пр.) с целью недопущения

дальнейших разрушительных действий, распространения вредоносных программ или утечки конфиденциальной информации.

Прекращение нападения и восстановление нормальной работы информационных систем может потребовать скоординированных действий не только самих сотрудников департамента информационной безопасности, но и:

- специалистов ИТ-подразделений, отвечающих за атакуемые информационные сервисы;
- пользователей атакованных информационных систем;
- предприятий-партнеров, имеющих отношение к атакованным информационным ресурсам;
- разработчиков и поставщиков атакованных информационных систем;
- поставщиков телекоммуникационных услуг, через которых осуществляется атака;
- сторонних консультантов, специализирующихся на соответствующих проблемах информационной безопасности.

Одним из наиболее важных обстоятельств работы на данном этапе является то, какими полномочиями обладает специалист (дежурный), отвечающий за реагирование на инциденты. В частности, необходимо заранее предусмотреть возможность оперативного самостоятельного отключения тех или иных информационных сервисов специалистами по реагированию на инциденты (самостоятельно, либо через соответствующее ИТ-подразделение). Особую важность имеет способность ответственных специалистов оперативно оценить ситуацию, провести ее анализ (в большинстве практических ситуаций это необходимо будет делать по неполным данным о нападающей стороне) и принять решение о приостановке работы тех или иных информационных сервисов, до выявления и устранения угроз и/или введения в действие дополнительных средств противодействия вторжениям. При принятии такого решения необходимо учитывать (как правило, на основе экспертных оценок) как возможный ущерб, который может быть вызван выявленным нарушением,

так и возможный ущерб от остановки информационных сервисов, которая (остановка) может быть осуществлена с целью предотвращения ущерба от действий нападающей стороны. Характерным примером такой ситуации является нападение на систему электронной торговли, когда нападающая сторона может нанести серьезный ущерб (похитить конфиденциальную информацию участников торговых сделок, самостоятельно совершить незаконные сделки от имени участников торговой системы и пр.), а остановка сервиса с целью предотвращения такого ущерба может привести к потерям, связанным с упущенной выгодой от несовершенных сделок и ущербом для деловой репутации. Другим примером такой ситуации является реагирование на распределенные атаки типа "отказ в обслуживании" (Distributed Deny of Service, DDoS), часто осуществляемые на серверы в сети Интернет, когда может быть необходимо на некоторое время полностью отключить сервер как в ущерб пользователям, так и в ущерб владельцам информационных ресурсов, расположенных на сервере.

Основой для принятия решений может быть заранее сформированный перечень (справочник) возможных основных инцидентов и признаков нарушений (проникновений), в котором может быть приведена оценка рисков суммарных потерь и рекомендованные действия для каждого типа нарушений (в том числе и перечень ситуаций, когда необходимо осуществить отключение сервисов во избежание утечки или нарушения целостности информации, являющейся наиболее критичной для всей деятельности предприятия).

4 Идентификация нападающего

Идентификация нападающего (или источника распространения вредоносных программ) является важным шагом в процессе реагирования, следующим непосредственно за локализацией нападения. В случае если нападение осуществлялось из локальной сети предприятия, при надлежащем соблюдении внутренних режимных правил эта задача может оказаться относительно легкой. В случае если нападение было совершено извне, задача

идентификации нападающих принципиально усложняется и в некоторых ситуациях проблема становится практически неразрешимой.

Как правило, для обнаружения источника нападения необходимо:

- детально изучить все технические аспекты нападения;
- провести качественный анализ процесса нападения в контексте функционирования атакуемой системы защиты информации;
- организовать взаимодействие со сторонними организациями, которые могут содействовать в идентификации нападающего.

Одной из наиболее важных задач анализа процесса нападения является установление той информации, которая была известна нападающим до начала нападения и которой они воспользовались для осуществления этого нападения. В частности, в процессе такого анализа с определенной степенью уверенности можно установить, что до начала нападения злоумышленникам были известны:

- информация о структуре и составе атакуемой информационной системы (используемые программные и аппаратные средства, их архитектура и используемые настройки);
- сведения о режиме работы организации и функционирования отдельных элементов информационной системы. Сведения о регламенте некоторых бизнес-процессов предприятия;
- конкретные идентификационные данные (имена пользователей, пароли), необходимые для проникновения в информационную систему и/или правила (алгоритмы) их генерации.

Обобщение всех этих сведений может помочь установить, какие контакты были у нападающих с атакуемой компанией (а каких не было), и, сопоставляя факты, а также пользуясь методом исключения, постараться ограничить круг лиц, которые потенциально могли быть причастны к организации данного инцидента.

В свою очередь, проведение такого анализа будет возможно только в том случае, если все информационные системы и системы защиты информации

настроены надлежащим образом (в частности, в них ведутся все необходимые системные журналы) и системные данные не были повреждены в процессе нападения.

Вторым важным направлением организационной и аналитической работы при установлении (идентификации) нападающих, совершивших нападение извне, является взаимодействие с администраторами систем (телекоммуникационных сетей, компьютеров, использовавшихся в качестве прокси-серверов, и пр.), с использованием которых было осуществлено нападение. Подходы к такому взаимодействию в каждом конкретном случае, скорее всего, будут индивидуальными и могут зависеть от политики раскрытия информации администрации той сети или узла, через который осуществлялась атака. Также могут быть предприняты действия для того, чтобы в судебном порядке или с привлечением правоохранительных органов обязать администрации таких сетей и узлов предоставить необходимую информацию, связанную с произошедшим нападением.

Процесс идентификации должен по возможности проводиться с учетом того, что впоследствии необходимо будет использовать информацию о нападающих как доказательство в уголовном процессе. В частности, при снятии (копировании) необходимых лог-файлов с атакованных компьютеров представителями правоохранительных органов, ведущими следствие по данному делу, должны быть соблюдены все процессуальные формальности, предусмотренные уголовно-процессуальным законодательством. Одной из особенностей процедуры изъятия доказательств у потерпевшей стороны в этом случае является то, что понятые, присутствующие при изъятии, должны по возможности иметь хотя бы общее представление о смысле производимой процедуры. Также на этом этапе при необходимости может быть проведена технико-криминалистическая экспертиза компьютерных систем.

5 Оценка и анализ процесса нападения и его обстоятельств

Одним из заключительных шагов процесса реагирования на инцидент является оценка и анализ процесса нападения и его обстоятельств. Этот анализ необходимо проводить в контексте целей и задач функционирования всего предприятия, с учетом результатов работы по идентификации лиц, совершивших нападение. Основные задачи аналитической работы на данном этапе:

- анализ целей и мотивов, нападавших;
- анализ фундаментальных (организационных и технических) причин, которые сделали нападение возможным и успешным (если оно было успешным);
- анализ последствий (в том числе и долгосрочных) нападения для всей деятельности предприятия;
- анализ и оценка работы персонала и взаимоотношений с предприятиями-партнерами (в том числе и с поставщиками информационных систем и средств защиты информации).

Результатом анализа должны быть выводы, которые могут послужить основой для организационной работы в различных направлениях:

- корректировка и уточнение политики информационной безопасности предприятия;
- проведение дополнительной работы с персоналом предприятия (наказания, поощрения, дополнительное обучение и пр.);
- проведение дополнительной работы с персоналом департамента информационной безопасности предприятия, а также персоналом ИТ-служб;
- пересмотр взаимоотношений с контрагентами предприятия (покупателями, поставщиками, партнерами по НИОКР и пр.), имеющими доступ к его защищаемой информации или информационным системам;
- привлечение сторонних консультантов по информационной безопасности и специалистов по средствам защиты информации;

– инициирование технического переоснащения отдельных участков информационной инфраструктуры предприятия.

Таким образом, анализ и всесторонняя оценка инцидентов является отправной точкой для реализации комплекса мер по совершенствованию системы обеспечения информационной безопасности на предприятии. Все эти меры должны в будущем снизить вероятность аналогичных инцидентов, а также уменьшить вероятность нанесения существенного ущерба в случае их повторения.

Важной составляющей анализа нападения также является оценка ущерба от произошедшего нарушения информационной безопасности. Ущерб может быть оценен одновременно с нескольких точек зрения и зависит от характера возникшей внештатной ситуации. Наиболее простым для количественной экономической оценки является прямой ущерб: затраты на восстановление утраченной информации (могут быть рассчитаны на основе трудоемкости работ по восстановлению информации и данных о средней стоимости рабочего времени соответствующих специалистов), затраты на замену скомпрометированных паролей, кодов и ключей, стоимость поврежденного оборудования, штрафные санкции за разглашение конфиденциальной информации (если такие санкции, например, были предусмотрены договорами с подрядчиками, поставщиками или заказчиками) и пр. Также в оценке нуждается упущенная выгода, которая может быть связана как с непосредственным прекращением (приостановкой, замедлением) текущих операций предприятия, так и с долгосрочным (перспективным) негативным влиянием возникшей внештатной ситуации – потерей доверия к предприятию, приводящей к оттоку заказчиков, формированием негативного имиджа предприятия и пр. Отдельно также может быть оценено падение рыночной стоимости предприятия – его акций (если речь идет о предприятии, акции которого котируются на биржевом рынке).

Наиболее сложным для оценки является моральный ущерб и последствия от разглашения информации личного характера (например, сведений,

составляющих врачебную тайну). Конкретные суммы морального ущерба, как правило, могут быть установлены по результатам судебных разбирательств с отдельными лицами, которым такой ущерб был нанесен, либо процедур досудебного урегулирования конфликтов (на основе требований пострадавших лиц).

6 Заключительные этапы процесса реагирования

Заключительным этапом процесса реагирования также является устранение негативных последствий нападения – локализация ущерба, причиненного произошедшим нарушением. Эта работа может включать в себя:

- смену скомпрометированных паролей отдельных пользователей;
- переустановку поврежденных операционных систем, а также поврежденного программного обеспечения;
- восстановление нарушенной конфигурации (настроек) программного обеспечения и операционных систем;
- восстановление поврежденной информации (баз данных, файлов), как из ранее созданных резервных копий, так и другими способами.

В процессе восстановления работоспособности информационных систем на некоторое время могут быть задействованы резервные (альтернативные) аппаратные и программные платформы.

Кроме того, необходимым завершающим шагом может быть дополнительная информационная работа, которая может в себя включать:

- рассылку пользователям информации о произошедших инцидентах (в виде специальных писем и бюллетеней);
- передачу некоторых сведений о нападении в средства массовой информации;
- передачу сведений о нападении крупным группам реагирования на инциденты, связанные с информационной безопасностью (таким как, например, CERT/CC), а также в научно-исследовательские центры, занимающиеся проблемами защиты информации;

– дополнительную информационную работу с поставщиками информационных систем и подрядчиками, осуществлявшими их поставку, внедрение и настройку.

С точки зрения распределения обязанностей по выполнению отдельных функций в рамках процесса реагирования на инциденты, одним из эффективных и достаточно широко используемых подходов к организации реагирования на инциденты является построение централизованной системы реагирования на инциденты, когда одна группа реагирования обслуживает несколько подразделений или предприятий. В частности, такой подход реализован в Министерстве обороны США (он был описан в одной из предыдущих лекций), где несколько централизованных групп реагирования на инциденты обслуживают множество войсковых подразделений. Централизованные группы реагирования могут создаваться для обслуживания различных предприятий и организаций. Это могут быть компании, входящие в крупный холдинг, организации, входящие в одну исследовательскую сеть, университеты и исследовательские организации одной страны, клиенты поставщика определенных продуктов или услуг и т.д. Для объединения усилий различных групп реагирования был создан специальный Форум групп реагирования на инциденты и обеспечения безопасности (Forum of Incident Response and Security Teams, FIRST), на интернет сайте которого (<http://www.first.org/>) можно найти полный список его участников. При этом все функции по реагированию не могут быть переданы в централизованную группу реагирования – в каждом конкретном случае необходимо детально разграничить полномочия, ответственность и функции, выполняемые предприятием самостоятельно, и функции, выполняемые централизованной группой. Договоренность между централизованной группой реагирования и группой реагирования (специалистами по безопасности) самого предприятия должна предусматривать не только разграничение функций, но и описывать основные процедуры взаимодействия в процессе реагирования на инцидент.

1 Цели аудитов информационной безопасности, их классификации по типам

Аудит состояния информационной безопасности на предприятии представляет собой экспертное обследование основных аспектов информационной безопасности, их проверку на соответствие определенным требованиям. В некоторых случаях под аудитом информационной безопасности подразумевается проверка защищенности отдельных элементов информационной инфраструктуры предприятия (сегментов его сети, отдельных серверов, баз данных, Интернет-сайтов и пр.) и надежности средств защиты информации (межсетевых экранов, систем обнаружения вторжений и пр.). Однако мы в дальнейшем исходим из того, что аудит информационной безопасности является комплексным (по возможности, исчерпывающим) исследованием всех аспектов информационной безопасности (как технических, так и организационных) в контексте всей хозяйственной деятельности предприятия с учетом действующей политики информационной безопасности, объективных потребностей предприятия и требований, предъявляемых третьими лицами (государством, контрагентами и пр.).

Различают два основных вида аудита: внутренний (проводимый исключительно силами сотрудников предприятия) и внешний (осуществляемый сторонними организациями).

Целями аудита могут быть:

- установление степени защищенности информационных ресурсов предприятия, выявление недостатков и определение направлений дальнейшего развития системы защиты информации;
- проверка руководством предприятия и другими заинтересованными лицами достижения поставленных целей в сфере информационной безопасности, выполнения требований политики безопасности;

- контроль эффективности вложений в приобретение средств защиты информации и реализацию мероприятий по обеспечению информационной безопасности;

- сертификация на соответствие общепризнанным нормам и требованиям в сфере информационной безопасности (в частности, на соответствие национальным и международным стандартам).

Одной из стратегических задач, решаемых при проведении аудита информационной безопасности и получении соответствующего сертификата, является демонстрация надежности предприятия, его способности выступать в качестве устойчивого партнера, способного обеспечить комплексную защиту информационных ресурсов, что может быть особенно важно при осуществлении сделок, предполагающих обмен конфиденциальной информацией, имеющей большую стоимость (финансовыми сведениями, конструкторско-технологической документацией, результатами НИОКР и пр.).

В том случае, если аудит является внутренним, группу аудиторов необходимо сформировать из числа таких специалистов, которые сами не являются разработчиками и администраторами используемых информационных систем и средств защиты информации и не имели отношения к их внедрению на данном предприятии.

Как правило, предприятие может прибегать к помощи внешних аудиторов с целью:

- повышения объективности, независимости и профессионального уровня проверки;

- получения заключений о состоянии информационной безопасности и соответствии международным стандартам от независимых аудиторов.

Компании, специализирующиеся на проведении аудитов, могут осуществлять проверки состояния информационной безопасности на соответствие таким общепризнанным стандартам и требованиям, как:

- ISO 15408: Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий);
- ISO 17799 (BS 7799): Code of Practice for Information Security Management (Практические правила управления информационной безопасностью);
- BSI\IT: Baseline Protection Manual (Руководство базового уровня по защите информационных технологий Агентства информационной безопасности Германии);
- COBIT: Control Objectives for Information and related Technology (Основные цели для информационных и связанных с ними технологий);
- Требованиям Руководящих документов ФСТЭК РФ, ФСБ или других государственных органов и других документов (таких как SAC, COSO, SAS 55/78).

При этом организация, осуществляющая внешний аудит, должна отвечать определенным требованиям:

- иметь право (лицензию) на выдачу заключений о соответствии определенным требованиям (например, аккредитацию UKAS – United Kingdom Accreditation Service);
- сотрудники должны иметь право доступа к информации, составляющей государственную и военную тайну (если такая информация имеется на проверяемом предприятии);
- обладать необходимыми программными и аппаратными средствами для исчерпывающей проверки имеющегося у предприятия программного и аппаратного обеспечения.

2 Этапы аудита

Основными этапами проведения аудита являются:

- инициирование проведения аудита;
- непосредственно осуществление сбора информации и проведение обследования аудиторами;
- анализ собранных данных и выработка рекомендаций;
- подготовка аудиторского отчета и аттестационного заключения.

Аудит должен быть инициирован руководством предприятия с достаточно четко сформулированной целью на определенном этапе развития информационной системы или системы обеспечения информационной безопасности предприятия (например, после завершения одного из этапов внедрения). В случае если аудит не является комплексным, на начальном этапе необходимо определить его непосредственные границы:

- перечень обследуемых информационных ресурсов и информационных систем (подсистем);
- перечень зданий, помещений и территорий, в пределах которых будет проводиться аудит;
- основные угрозы, средства защиты от которых необходимо подвергнуть аудиту;
- элементы системы обеспечения информационной безопасности, которые необходимо включить в процесс проверки (организационное, правовое, программно-техническое, аппаратное обеспечение);

Основная стадия – проведение аудиторского обследования и сбор информации – как правило, должно включать в себя:

- анализ имеющейся политики информационной безопасности и другой организационной документации;
- проведение совещаний, опросов, доверительных бесед и интервью с сотрудниками предприятия;

- проверку состояния физической безопасности информационной инфраструктуры предприятия;
- техническое обследование информационных систем – программных и аппаратных средств (инструментальная проверка защищенности).

Прежде чем приступить собственно к аудиту информационной безопасности, аудиторам (в частности, если проводится внешний аудит) необходимо ознакомиться со структурой предприятия, его функциями, задачами и основными бизнес-процессами, а также с имеющимися информационными системами (их составом, функциональностью, процедурами использования и ролью на предприятии). На начальном этапе аудиторы принимают решения о том, насколько глубоко и детально будут исследованы отдельные элементы информационной системы и системы защиты информации. Также необходимо заранее скоординировать с пользователями информационных систем процедуры проверки и тестирования, требующие ограничения доступа пользователей (такие процедуры по возможности должны проводиться в нерабочее время или в периоды наименьшей загрузки информационной системы).

Качественный анализ действующей на предприятии политики безопасности является отправной точкой для проведения аудита. Одна из первых задач комплексного аудита – установление того, в какой степени действующая политика соответствует объективным потребностям данного предприятия в безопасности, могут ли действия в рамках данной политики обеспечить необходимый уровень защищенности информации и средств ее обработки, хранения и передачи. Это, в свою очередь, может потребовать проведения дополнительной оценки значимости основных информационных активов предприятия, их уязвимости, а также существующих рисков и угроз. Анализ политики также может включать оценку таких ее характеристик, как:

Тема 2.7 – Аудит информационной безопасности
(Управление информационной безопасностью)

- полнота и глубина охвата всех вопросов, а также соответствие содержания политик нижнего уровня целям и задачам, установленным в политиках верхнего уровня;
- понятность текста политики для людей, не являющихся техническими специалистами, а также четкость формулировок и невозможность их двойного толкования;
- актуальность всех положений и требований политики, своевременность учета всех изменений, происходящих в информационных системах и бизнес-процессах.

После проверки основных положений политики безопасности в процессе аудита могут быть изучены (проверены) действующие классификации информационных ресурсов по степени критичности и конфиденциальности, а также другие документы, имеющие отношение к обеспечению информационной безопасности:

- организационные документы подразделений предприятия (положения об отделах, должностные инструкции);
- инструкции (положения, методики), касающиеся отдельных бизнес-процессов предприятия;
- кадровая документация, обязательства о неразглашении сведений, данные сотрудниками, свидетельства о прохождении обучения, профессиональной сертификации, аттестации и ознакомлении с действующими правилами;
- техническая документация и пользовательские инструкции для различных используемых программных и аппаратных средств (как разработанных самим предприятием, так и приобретенных у сторонних поставщиков): межсетевых экранов, маршрутизаторов, операционных систем, антивирусных средств, систем управления предприятием и пр.

Основная работа аудиторов в процессе сбора информации заключается в изучении фактически предпринимаемых мер по обеспечению защиты информационных активов предприятия, таких как:

- организация процесса обучения пользователей приемам и правилам безопасного использования информационных систем;
- организация работы администраторов информационных и телекоммуникационных систем и систем защиты информации (правильность использования программных и аппаратных средств администрирования, своевременность создания и удаления учетных записей пользователей, а также настройки их прав в информационных системах, своевременность замены паролей и обеспечение их соответствия требованиям безопасности, осуществление резервного копирования данных, ведение протоколов всех производимых в процессе администрирования операций, принятие мер при выявлении неисправностей и пр.);
- организация процессов повышения квалификации администраторов информационных систем и систем защиты информации;
- обеспечение соответствия необходимых (в соответствии с политикой безопасности и должностными обязанностями) прав пользователей информационных систем и фактически имеющихся;
- организация назначения и использования специальных («суперпользовательских») прав в информационных системах предприятия;
- организация работ и координации действий при выявлении нарушений информационной безопасности и восстановлении работы информационных систем после сбоев и нападений (практическое выполнение «аварийного плана»);
- предпринимаемые меры антивирусной защиты (надлежащее использование антивирусных программ, учет всех случаев заражения, организация работы по устранению последствий заражений и пр.);

Тема 2.7 – Аудит информационной безопасности
(Управление информационной безопасностью)

- обеспечение безопасности приобретаемых программных и аппаратных средств (наличие сертификатов и гарантийных обязательств, поддержка со стороны поставщика при устранении выявленных недостатков и пр.);
- обеспечение безопасности самостоятельно разрабатываемого программного обеспечения (наличие необходимых требований в проектной документации информационных систем, качество программной реализации механизмов защиты и пр.);
- организация работ по установке и обновлению программного обеспечения, а также контроля за целостностью установленного ПО;
- предпринимаемые меры по обеспечению учета и сохранности носителей информации (дисков, дискет, магнитных лент и пр.), а также по их безопасному уничтожению после окончания использования;
- эффективность организации взаимодействия сотрудников предприятия – пользователей информационных систем – со службой информационной безопасности (в частности, по вопросам реагирования на инциденты и устранения их последствий).

Одним из важных направлений аудиторской проверки является контроль того, насколько своевременно и полно положения и требования политики безопасности и других организационных документов доводятся до персонала предприятия. В том числе, необходимо оценить, насколько систематически и целенаправленно осуществляется обучение персонала (как при занятии должностей, так и в процессе работы), и, соответственно, дать оценку тому, в какой мере персонал понимает все предъявляемые к нему требования, осознает свои обязанности, связанные с обеспечением безопасности, а также возможную ответственность, которая может наступить при нарушении установленных требований.

В процесс проведения интервью, совещаний и бесед с персоналом необходимо включить как можно больше сотрудников предприятия, имеющих

хотя бы какое-то отношение к информационным системам и процедурам обработки информации: администраторов и разработчиков информационных систем, операторов и других пользователей, вспомогательный персонал и пр. При непосредственной работе с персоналом аудиторам необходимо выяснить особенности протекания отдельных бизнес-процессов, роли отдельных сотрудников в этих процессах и их потенциальные возможности влиять на информационную безопасность. Также необходимо оценить, в какой мере сотрудники фактически выполняют свои обязанности в отношении обеспечения информационной безопасности.

Одной из важных задач аудита может быть установление того, насколько предприятие способно противодействовать внутренним угрозам в лице сотрудников, целенаправленно действующих, чтобы нанести тот или иной ущерб предприятию и имеющих для этого различные возможности. В частности, для этого могут быть исследованы:

- процедуры отбора и принятия новых сотрудников на работу, а также их предварительной проверки;
- процедуры контроля за деятельностью сотрудников (отслеживания их действий);
- процедуры регистрации пользователей и назначения им прав в информационных системах;
- распределение функций между различными сотрудниками и минимизация их привилегий, а также возможное наличие избыточных прав у некоторых пользователей и администраторов.

3 Проверка состояния физической безопасности информационной инфраструктуры

Проверка состояния физической безопасности информационной инфраструктуры, как правило, включает в себя:

- проверку того, чтобы наиболее важные объекты информационной инфраструктуры и системы защиты информации располагались в зонах (частях

зданий, помещениях), имеющих пропускной режим, а также оборудованных камерами видеонаблюдения и другими средствами контроля (электронными замками, средствами биометрической идентификации и пр.);

- проверку наличия и работоспособности технических средств, обеспечивающих устойчивую работу компьютерного и телекоммуникационного оборудования: источников бесперебойного энергоснабжения, кондиционеров (там, где это необходимо) и пр.;

- проверку наличия и работоспособности средств пожарной сигнализации и пожаротушения;

- проверку распределения ответственности за физическое (техническое) состояние объектов информационной инфраструктуры предприятия.

4 Инструментальная проверка защищенности

Инструментальная проверка защищенности является в основном технической задачей и осуществляется с использованием специализированного программного обеспечения, которое подключается к информационной системе предприятия и автоматически производит сбор всевозможных сведений: версий установленных операционных систем и программного обеспечения, данных об используемых сетевых протоколах, номеров открытых портов, данных о версиях установленных обновлений и пр. К другим направлениям инструментального и технического контроля также относятся такие работы, как:

- непосредственное изучение работы отдельных серверов, рабочих станций и сетевого оборудования соответствующими техническими специалистами, которые могут проверить различные аспекты их функционирования (процедуры загрузки, выполняемые процессы, содержимое конфигурационных файлов и пр.);

- сбор и последующий анализ данных о том, как выполняются процедуры резервного копирования, а также другие необходимые технические процедуры, предусмотренные регламентом;

- проверка качества программного обеспечения, самостоятельно разработанного предприятием (в том числе и путем анализа исходных кодов и проектной документации к нему), выявление ошибок, которые могут стать причиной сбоев, несанкционированных проникновений, разрушения и утечки информации и других инцидентов;
- изучение работы сети (сетевого трафика, загрузки различных сегментов сети и пр.);
- проведение с целью тестирования пробных, контролируемых «нарушений» информационной безопасности (по возможности без нанесения реального вреда и во внерабочее время), таких как атаки типа «отказ в обслуживании» (DoS) или проникновение в определенные базы данных и на определенные серверы, а также использование различных известных уязвимостей с целью выяснения конкретных параметров безопасности, устойчивости и надежности проверяемой информационной системы.

Также в процессе аудита может быть проверено ведение журналов (лог-файлов) информационных систем и применение других инструментов сбора и анализа информации, необходимых для обеспечения текущего контроля за соблюдением требований информационной безопасности и своевременного реагирования на инциденты (средств обнаружения вторжений, анализаторов работы локальных сетей и пр.). Информация, накопленная в лог-файлах за время использования информационных систем, является одним из важных объектов анализа в процессе аудита. На основе этих данных могут быть сделаны оценки и выводы относительно соблюдения установленных правил использования информационных систем, эффективности используемых средств защиты информации, поведения пользователей, а также о потенциально возможных проблемах.

5 Анализ информации

Анализ всей информации, полученной в процессе ознакомления с документацией, контроля фактического выполнения всех установленных требований, получения сведений от сотрудников, изучения работы аппаратных средств и программного обеспечения, проверки физической защищенности и проведения инструментальных проверок должен быть произведен с учетом выявленных рисков и потребностей предприятия в информационной безопасности. В частности, такой анализ предполагает выявление конкретных особенностей программных и аппаратных средств, бизнес-процедур, организационных правил и распределений функциональных обязанностей и полномочий, которые могут негативно повлиять на обеспечение информационной безопасности, а также описание причинно-следственных взаимосвязей между выявленными особенностями функционирования предприятия и увеличением рисков нарушения информационной безопасности. Все исследованные обстоятельства, выявленные недостатки и особенности должны быть обобщены, и таким образом должно быть сформировано общее представление о состоянии информационной безопасности на предприятии, отражены основные достоинства и недостатки действующей системы защиты информационных ресурсов, а также обозначены основные приоритеты и направления ее дальнейшего развития и совершенствования.

Результаты анализа могут быть представлены как в виде обобщенных кратких формулировок, характеризующих защищенность информации предприятия (адресованных руководству и собственникам предприятия), так и в виде перечня конкретных замечаний и предложений, относящихся к отдельным участкам работы (адресованных руководителю департамента информационной безопасности, руководителю службы безопасности, функциональным директорам и руководителям структурных подразделений предприятия).

Окончательным результатом анализа и обобщения данных, полученных в процессе аудита, является отчет (заключение), который может включать в себя:

- оценку состояния (уровня) защищенности информационных ресурсов и информационных систем;
- заключения о практическом выполнении требований, предусмотренных политикой информационной безопасности предприятия и иными требованиями, и документами;
- заключение о степени соответствия фактического уровня информационной безопасности требованиям определенных стандартов и нормативных документов;
- предложения по усовершенствованию политики информационной безопасности и реализации дополнительных практических мероприятий в этой сфере (как организационных, так и технических), а также о тех мерах, которые необходимо реализовать для прохождения сертификации на соответствие определенному стандарту (если по результатам проведенного аудита сделан вывод о том, что текущий уровень защищенности информационных ресурсов предприятия не соответствует таким требованиям);
- заключение о степени соответствия политики безопасности предприятия и всего комплекса мер по защите информации требованиям действующего законодательства и ведомственных нормативных актов;
- оценки экономической эффективности вложений в те или иные средства защиты информации, а также организационные мероприятия (отдачи от них);
- количественная (денежная) оценка возможных потерь от тех или иных нарушений, которые могут произойти при существующем уровне обеспечения информационной безопасности, а также расчет необходимых вложений, которые необходимо осуществить для достижения определенного уровня защищенности.

Также по результатам аудита могут быть сформулированы дополнительные рекомендации, касающиеся:

- пересмотра отдельных бизнес-процессов и процедур;

Тема 2.7 – Аудит информационной безопасности
(Управление информационной безопасностью)

- совершенствования работы с персоналом предприятия;
- внедрения и использования современных технических (программных и аппаратных) средств обработки и защиты информации;
- организации работы по защите информации;
- выбора приоритетов в процессе устранения существующих недостатков.

1 Применение программных средств управления безопасностью

Деятельность по обеспечению информационной безопасности на предприятии может поддерживаться программными продуктами различных типов. В большинстве случаев программная поддержка реализации политики информационной безопасности обеспечивается функциями и программными модулями, которые встроены непосредственно в программное обеспечение, создающее условия для хранения, обработки и передачи информации (операционные системы, системы управления базами данных, системы электронной почты, MRP/ERP-системы). Практически все современные программные продукты имеют внутренние средства, позволяющие четко определить права тех или иных пользователей, разграничить доступ к информации, распределить использование системных ресурсов и ввести другие ограничения, которые в целом должны обеспечить соблюдение установленных требований и реализацию политики информационной безопасности.

Применение других инструментальных средств, как правило, не является обязательным, но во многих случаях позволяет повысить эффективность и качество многих работ, связанных с оценкой рисков, разработкой организационной документации, контролем за выполнением установленных требований и выполнением многих других важных функций. Таким образом, выделяется отдельный класс специальных программных продуктов, предназначенных исключительно для поддержания процессов разработки политик безопасности и управления информационной безопасностью на организационном уровне. Основными функциями таких программ являются справочно-информационная поддержка, помощь при обработке управленческой информации, оценке рисков и подготовке необходимых документов. В частности, для этих целей может использоваться ПО следующих основных видов:

- сборники (интерактивные электронные справочники), которые содержат типовые документы (шаблоны документов), используемые для

Тема 2.8 – Программные средства планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

управления информационной безопасностью, описания отдельных процессов и процедур, связанных с обеспечением информационной безопасности, должностных обязанностей и функций сотрудников предприятия;

- системы, предназначенные для накопления и обработки сведений о рисках и проведения сводных оценочных расчетов показателей риска;

- ПО, интегрированное в информационную систему предприятия и позволяющее автоматически контролировать соблюдение установленных политик безопасности, а также помогающее формировать заключения о текущем состоянии информационной безопасности (в т.ч. путем анализа действий пользователей в информационной системе, а также путем анализа журналов операционных систем, программ, средств защиты и сетевого оборудования);

- ПО, осуществляющее поддержку процессов аудита информационной безопасности.

Также с управлением информационной безопасностью связаны программные продукты, которые:

- автоматически (централизованно и унифицировано) управляют учетными записями и правами доступа одновременно в нескольких элементах информационной инфраструктуры (базах данных, приложениях и пр.);

- производят автоматическое сканирование отдельных элементов информационной инфраструктуры (операционных систем, программ, средств защиты информации) и их проверку на устойчивость и наличие уязвимостей;

- производят автоматическое обновление программных продуктов с целью устранения выявленных уязвимостей (установку т.н. «патчей», «заплаток»).

2 Программная поддержка политики безопасности

Сборники (справочники), которые содержат типовые документы, связанные с обеспечением информационной безопасности, могут включать в себя:

- образцы политик безопасности разных уровней для предприятий, функционирующих в различных сферах деятельности и предъявляющих различные требования к уровню защищенности информации;
- образцы (шаблоны, бланки) документов, используемых в процессах защиты информации (обязательств о неразглашении информации, отчетов о состоянии информационной безопасности и пр.);
- образцы разделов различных договоров (контрактов с различными контрагентами или трудовых договоров с сотрудниками предприятия), содержащие требования к обеспечению информационной безопасности.

Такого рода электронные справочники могут выпускаться как на основе оригинальных методических разработок, так и на основе общепризнанных стандартов (таких как ISO 17799) с целью содействовать прохождению сертификации на соответствие этим стандартам. Выпускаемые электронные справочники могут быть дополнены учебниками, текстами стандартов и другими методическими материалами, выпущенными в виде брошюр. Одним из наиболее полных является электронный справочник «Information Security Policies Made Easy» американской компании Information Shield, Inc. Девятая версия этого справочника содержит более 1360 образцов и шаблонов различных документов, созданных с учетом требований стандарта ISO 17799 и относящихся ко всем аспектам информационной безопасности предприятия.

Концепции более развитых программных продуктов, основанных на интерактивном интеллектуальном анализе и совершенствовании политики безопасности, предполагают, что пользователь (менеджер) сначала внесет всю необходимую информацию о состоянии информационной безопасности на своем предприятии (ответит на задаваемые программой вопросы), а затем

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

получит детальный отчет о состоянии информационной безопасности, описание уровня соответствия требованиям стандартов, рекомендации по усовершенствованию действующей политики безопасности и другие отчеты. Таким образом, программное обеспечение позволяет увязывать в единый процесс процедуры первичного сбора информации о предприятии, анализа фактического уровня организационного обеспечения информационной безопасности, разработки документации, адаптации методов управления к определенным требованиям (например, стандарта ISO 17799) и проведение аудитов информационной безопасности.

Одним из таких программных продуктов является система «COBRA», поставляемая британской компанией «C&A Systems Security Ltd.» в двух вариантах: сокращенная версия включает в себя модуль «COBRA ISO17799 Consultant», а полная версия, помимо него, содержит также дополнительные средства анализа рисков («Risk Consultant») и специальный модуль, позволяющий создавать и модифицировать собственные базы знаний и наборы вопросов для исследования состояния информационной безопасности («Module Manager»). Базовый модуль этой системы предназначен для оценки того, в какой степени работа по защите информационной безопасности соответствует требованиям стандарта ISO 17799. На первом этапе его использования вступает в работу «Question Module» – Модуль ответов на вопросы, который содержит набор вопросов, разделенных на группы в соответствии со структурой стандарта ISO 17799: безопасность персонала, политика безопасности, управление доступом, планирование непрерывной работы и пр. (Рисунок 1).

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

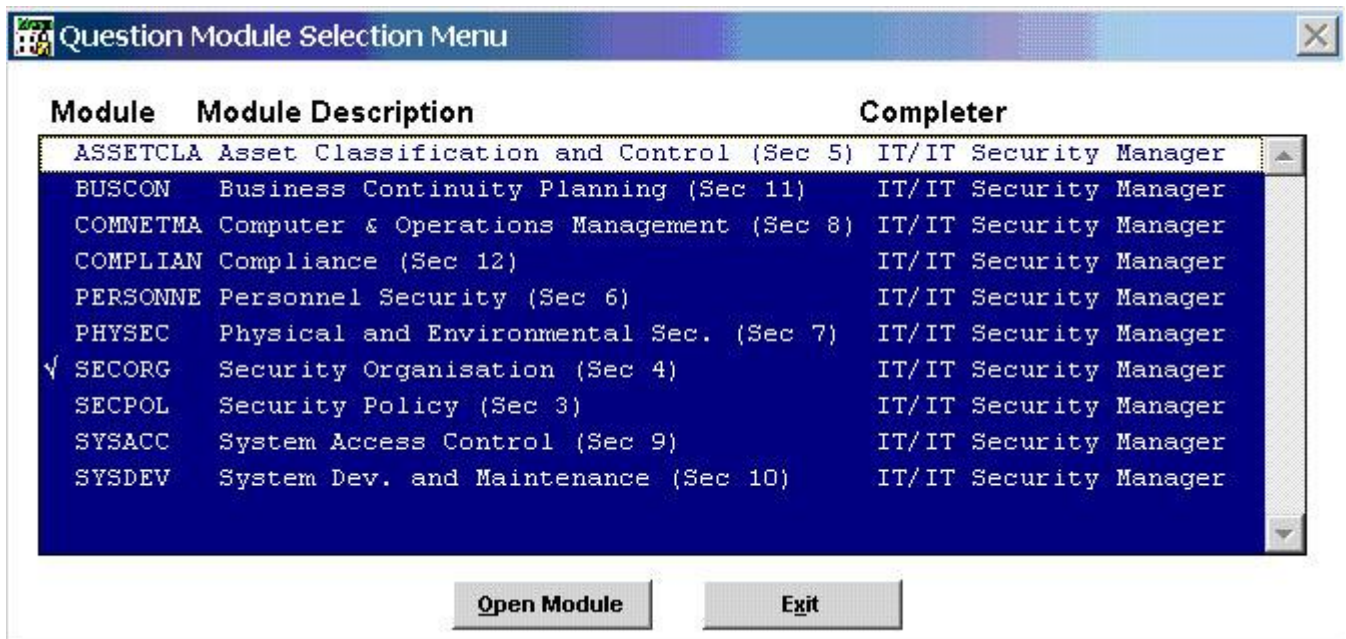


Рисунок 1 – Группы вопросов для анализа состояния ИБ системой «COBRA»

На основе введенной таким образом информации может быть получен отчет о состоянии информационной безопасности и степени ее соответствия требованиям стандарта. В частности, такой отчет может состоять из пяти основных разделов:

- 1) Вводная часть.
- 2) Перечень основных направлений работы, подвергнутых проверке.
- 3) Оценка уровня несоответствий
- 4) Перечень организационных мероприятий, реализация которых необходима для выполнения требований стандарта.
- 5) Перечень заданных вопросов и данных на них ответов.

Помимо текстовой части, в отчет также могут быть включены графики, наглядно отражающие уровни выполнения требований стандарта (Рисунок 2).

Дополнительные модули, входящие в полную версию программного продукта, необходимы для обеспечения более полного и гибкого анализа рисков в условиях конкретного предприятия.

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

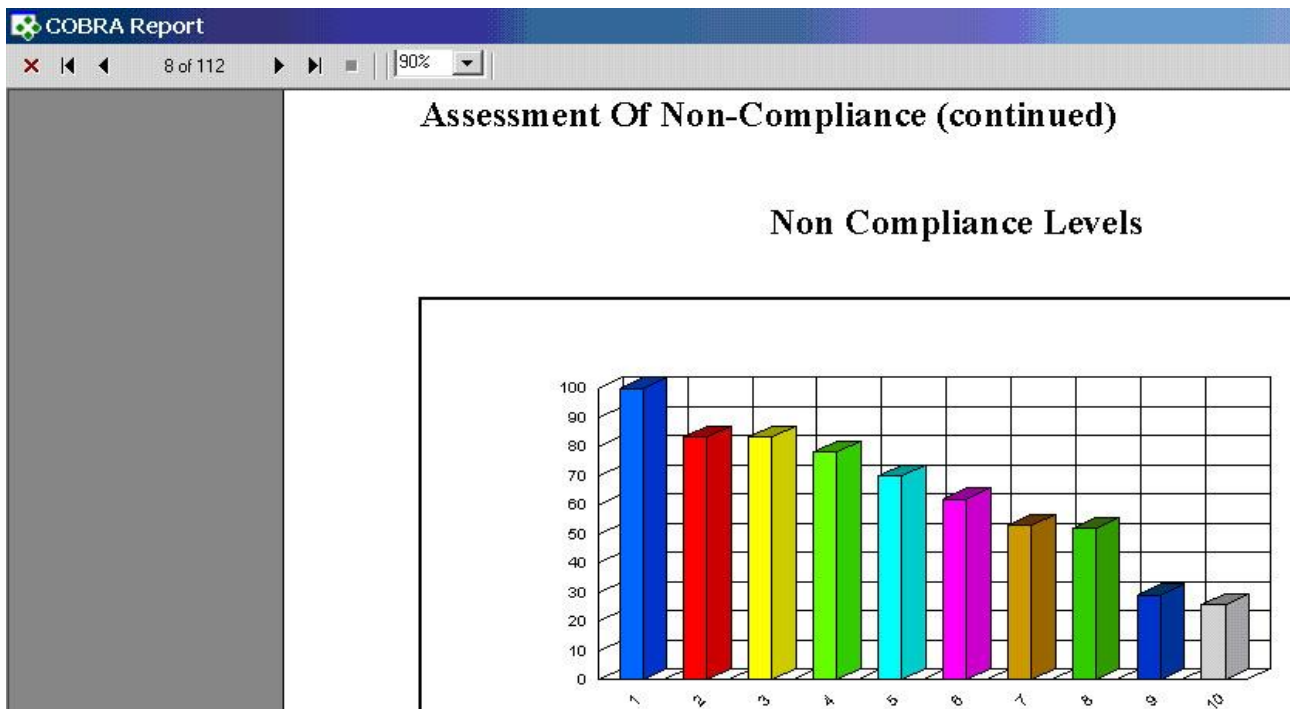


Рисунок 2 – График выполнения требований стандарта

The screenshot displays the COBRA Report interface. The title bar reads 'COBRA Report'. Below it, a navigation bar shows '15 of 112' and a zoom level of '90%'. The main content area is titled 'Improvements Required (continued)'. Below this title is a table with two columns: 'NUMBER' and 'TEXT'. The table lists three items, each with a number and a description of a required improvement. The first item is under the 'Risk Category: System Access Control'.

| NUMBER | TEXT |
|---|--|
| <i>Risk Category: System Access Control</i> | |
| 71 | Business requirements for access control should be defined and documented. (9.1.1) |
| 72 | There should be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services. Access to multi-user information services should be controlled through a formal user registration process. (9.2.1) |
| 73 | The allocation and use of privileges (any feature or facility of a multi-user information system that enables the user to override system or application controls) should be restricted and controlled. (9.2.2) |

Рисунок 3 – Раздел отчета о состоянии информационной безопасности

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

К числу программных продуктов такого рода, аналогичных британской системе «COBRA», относится также «Программный комплекс управления политикой информационной безопасности компании КОНДОР+», поставляемый Санкт-Петербургской фирмой «Диджитал Секьюрити». Он содержит как электронные справочники, так и *модуль*, осуществляющий интерактивное взаимодействие с пользователем в процессе анализа и совершенствования политики информационной безопасности. Данный программный комплекс, помимо сборника типовых политик безопасности, включает в себя четыре основных функциональных модуля (раздела):

- 1) «Проект» – предназначен для сбора информации о состоянии информационной безопасности.
- 2) «Отчеты» – предназначен для детального анализа состояния информационной безопасности на основе введенных данных.
- 3) «Диаграммы/статистика» – предназначен для сводного анализа состояния информационной безопасности.
- 4) «Анализ рисков» – предназначен для количественной оценки существующих рисков.

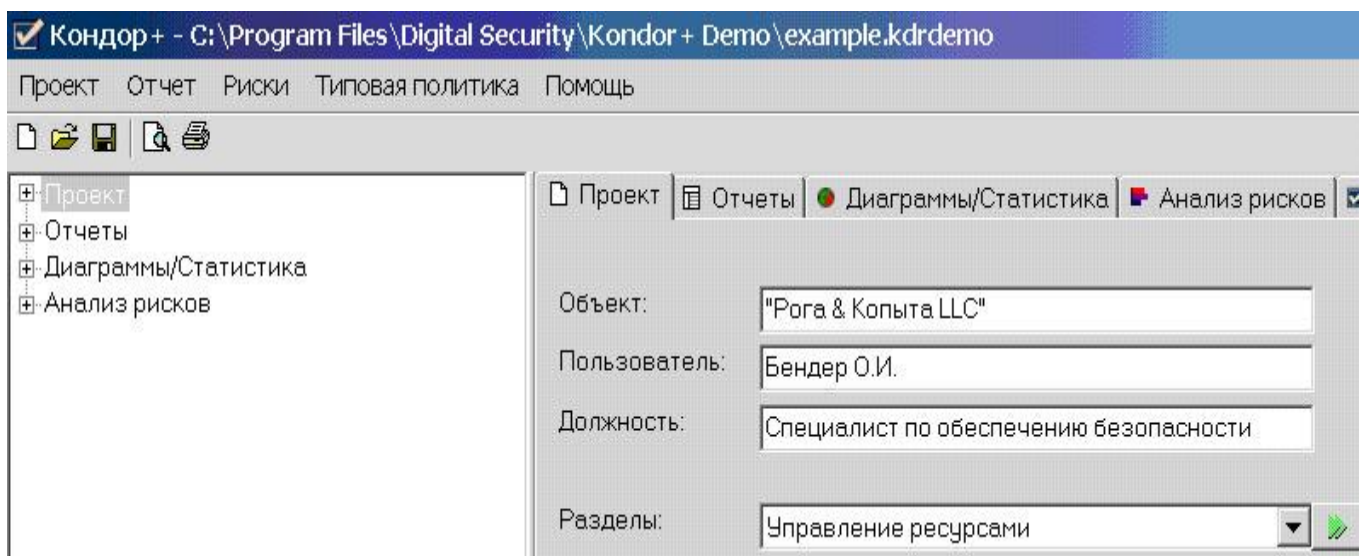


Рисунок 4 – Основные модули «Программного комплекса КОНДОР+»

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

Кондор+ - C:\Program Files\Digital Security\Kondor+ Demo\example.kdrdemo

Проект Отчет Риски Типовая политика Помощь

Проект

- Политика безопасности (0/10)
- Организационные меры (15/15)
 - Существуют ли в компании форумы
 - Какие вопросы, связанные с поли
 - Существуют ли в компании форумы
 - Рассматривается ли на этом фору
 - Рассматривается ли на этом фору
 - Является ли одной из поставлен
 - Рассматривается ли на этом фору
 - Рассматривается ли на этом фору
 - Проводится ли на этом форуме в
 - Существует ли в ИС распределен
 - Определены ли ресурсы по кажды

Проект | Отчеты | Диаграммы/Статистика | Анализ рисков | Демо-версия

Существуют ли в компании форумы по координации вопросов, связанных с обеспечением информационной безопасности?

☐ Да

☒ Нет

Рисунок 5 – Модуль «Проект» – ответы на вопросы о состоянии ИБ

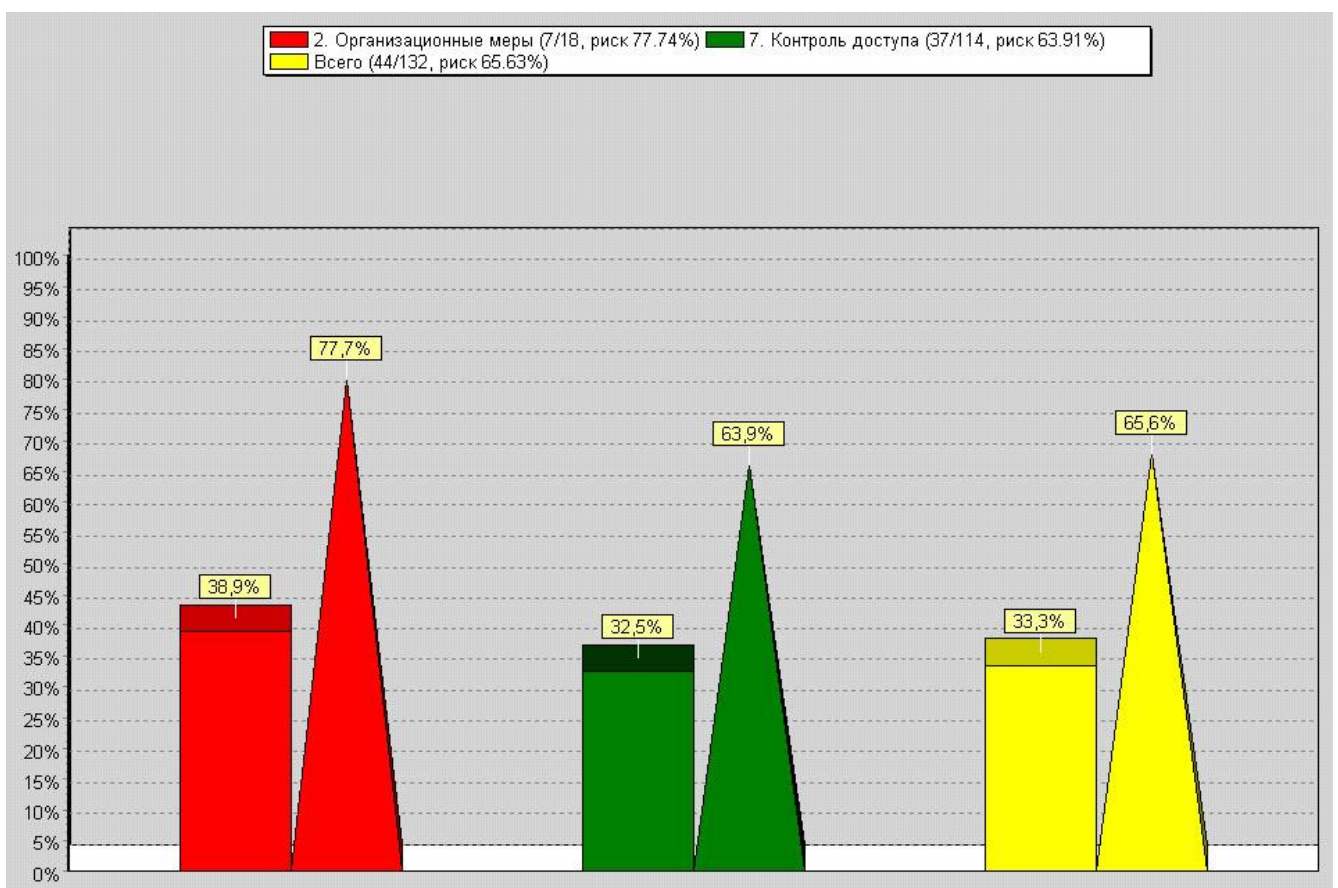


Рисунок 6 – Графическое представление сводных данных об имеющихся несоответствиях

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

Так же, как и в системе «COBRA», в модуле «Проект» «Программного комплекса КОНДОР+» пользователю – ответственному менеджеру – предлагается ответить на вопросы, сгруппированные в соответствии со структурой стандарта ISO 17799 и имеющие определенные варианты ответов.

На основе введенной таким образом информации программа автоматически формирует как сводную статистику, представляемую в виде диаграмм для каждого раздела стандарта ISO 17799, так и детализированные отчеты об имеющихся несоответствиях.

При анализе несоответствий в модуле «Отчеты» пользователь имеет возможность при помощи справочной подсистемы обратиться к комментариям и рекомендациям экспертов, описывающим отдельные вопросы практического применения стандарта ISO 17799.

Таким образом, программный комплекс «КОНДОР+» позволяет провести весь комплекс работ по сбору сведений о состоянии информационной безопасности и организации защитных мер на предприятии, сопоставлению фактического положения дел с требованиями стандарта ISO 17799 (как укрупненно, так и детально) и определению приоритетных направлений дальнейшего развития системы менеджмента.

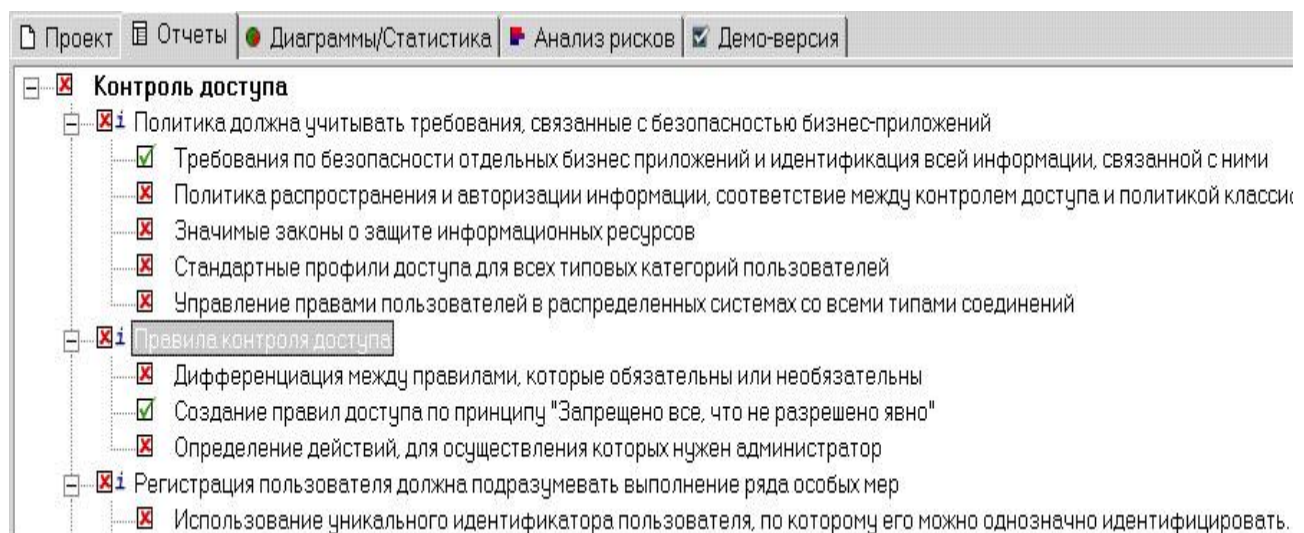


Рисунок 7 – Графическое представление сводных данных об имеющихся несоответствиях

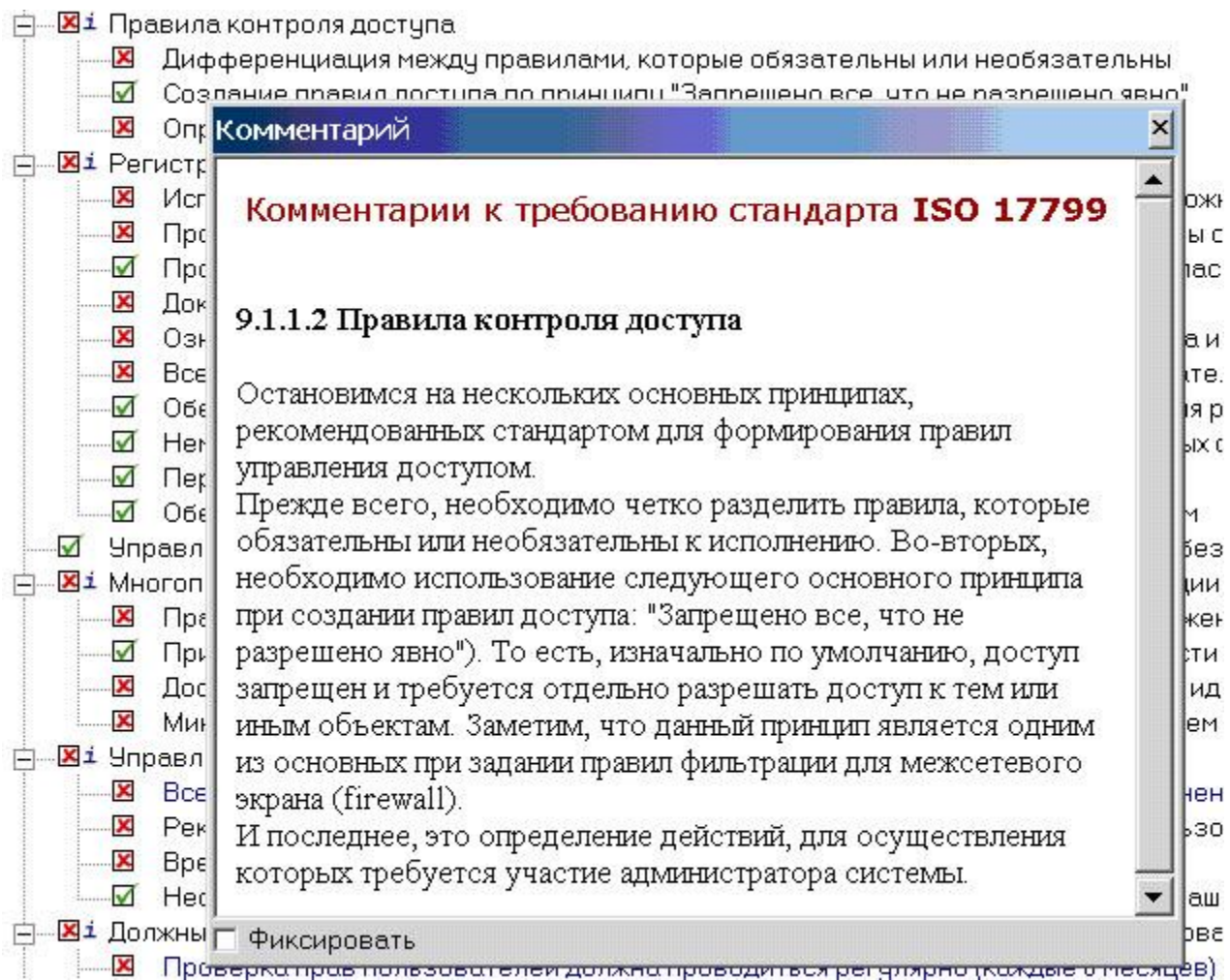


Рисунок 8 – Вызов экспертного комментария по определенному вопросу

3 Программная поддержка анализа рисков

Анализ рисков для информационной безопасности (как количественный, так и качественный), представляет собой одну из наиболее сложных задач в общей системе организационной и аналитической работы. Методологии анализа рисков и программные средства, реализующие эти методологии, как правило, предполагают выполнение следующих основных шагов, необходимых для формирования комплексной оценки существующих рисков:

- сбор информации об объектах защиты;
- выявление и оценка возможных угроз и уязвимостей;
- формирование сводной оценки рисков.

В большинстве случаев конечной целью такого анализа является формализованная оценка потребности предприятия в безопасности и

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

определение основных приоритетов развития системы защиты информации, а также создание информационной базы для оценки экономической эффективности вложений в реализацию отдельных мероприятий по обеспечению информационной безопасности.

Одним из инструментальных средств анализа рисков является семейство программных продуктов «CRAMM», поставляемых британской компанией «Insight Consulting»: «CRAMM Expert» и «CRAMM Express». Данный программный пакет основан на одноименной методике анализа рисков (CCTA Risk Analysis and Management Method – CRAMM), разработанной в 1985-1987 годах Центральным агентством по компьютерам и телекоммуникациям (Central Computer and Telecommunications Agency – CCTA) Великобритании и в дальнейшем переданной в ведение Службы безопасности Великобритании. Первую коммерческую версию программного продукта, который автоматизирует аналитические процедуры, осуществляемые в соответствии с методом CRAMM, CCTA выпустила в 1988 году, а его четвертая версия была выпущена в 2001 году уже компанией Insight Consulting.

Использование системы CRAMM включает в себя несколько последовательных этапов:

- изучение всех элементов анализируемой информационной системы;
- оценка угроз для информационной системы;
- сводный анализ рисков; принятие мер к устранению выявленных недостатков (Рисунок 9).

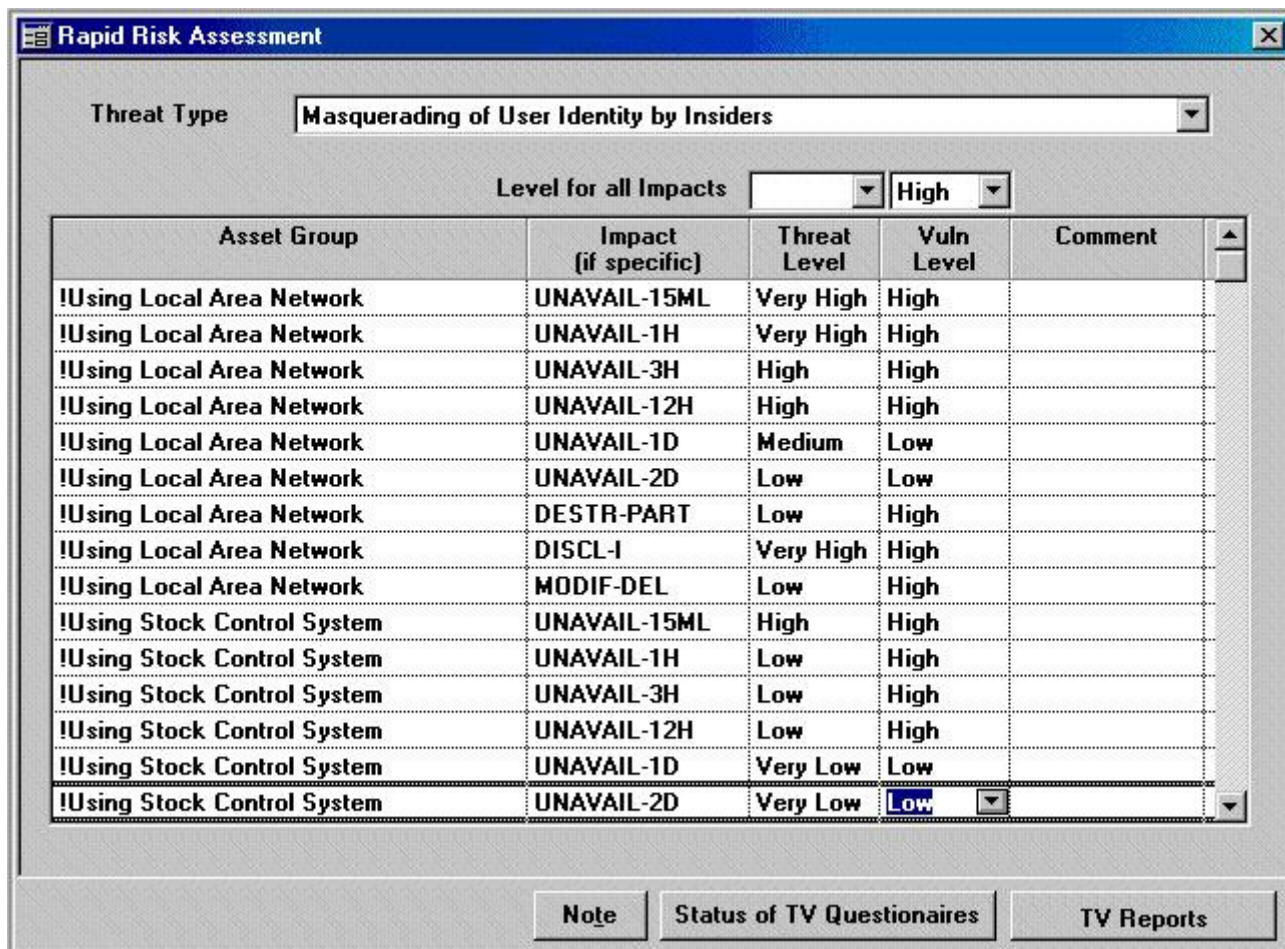
Тема 2.8 – Программные средства планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)



Рисунок 9 – Схема применения системы CRAMM

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)



| Asset Group | Impact (if specific) | Threat Level | Vuln Level | Comment |
|-----------------------------|----------------------|--------------|------------|---------|
| !Using Local Area Network | UNAVAIL-15ML | Very High | High | |
| !Using Local Area Network | UNAVAIL-1H | Very High | High | |
| !Using Local Area Network | UNAVAIL-3H | High | High | |
| !Using Local Area Network | UNAVAIL-12H | High | High | |
| !Using Local Area Network | UNAVAIL-1D | Medium | Low | |
| !Using Local Area Network | UNAVAIL-2D | Low | Low | |
| !Using Local Area Network | DESTR-PART | Low | High | |
| !Using Local Area Network | DISCL-I | Very High | High | |
| !Using Local Area Network | MODIF-DEL | Low | High | |
| !Using Stock Control System | UNAVAIL-15ML | High | High | |
| !Using Stock Control System | UNAVAIL-1H | Low | High | |
| !Using Stock Control System | UNAVAIL-3H | Low | High | |
| !Using Stock Control System | UNAVAIL-12H | Low | High | |
| !Using Stock Control System | UNAVAIL-1D | Very Low | Low | |
| !Using Stock Control System | UNAVAIL-2D | Very Low | Low | |

Рисунок 10 – Оценка взаимосвязей между различными угрозами и информационными сервисами в системе CRAMM

На основе всех введенных данных и по результатам расчетов и обработки информации могут быть получены сводные характеристики уровней риска для анализируемой информационной системы и, в частности, для отдельных информационных сервисов (Рисунок 11).

После того как произведена оценка рисков, система предлагает реализовать конкретные меры по повышению уровня защищенности, используя введенную информацию о состоянии информационной безопасности, а также собственную «Библиотеку контрмер» – базу знаний, которая содержит примеры и рекомендации (как конкретные, так и общие), относящиеся к различным аспектам защиты информационных ресурсов. С их применением может быть начат переход от анализа рисков к непосредственным управленческим действиям по обеспечению информационной безопасности:

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

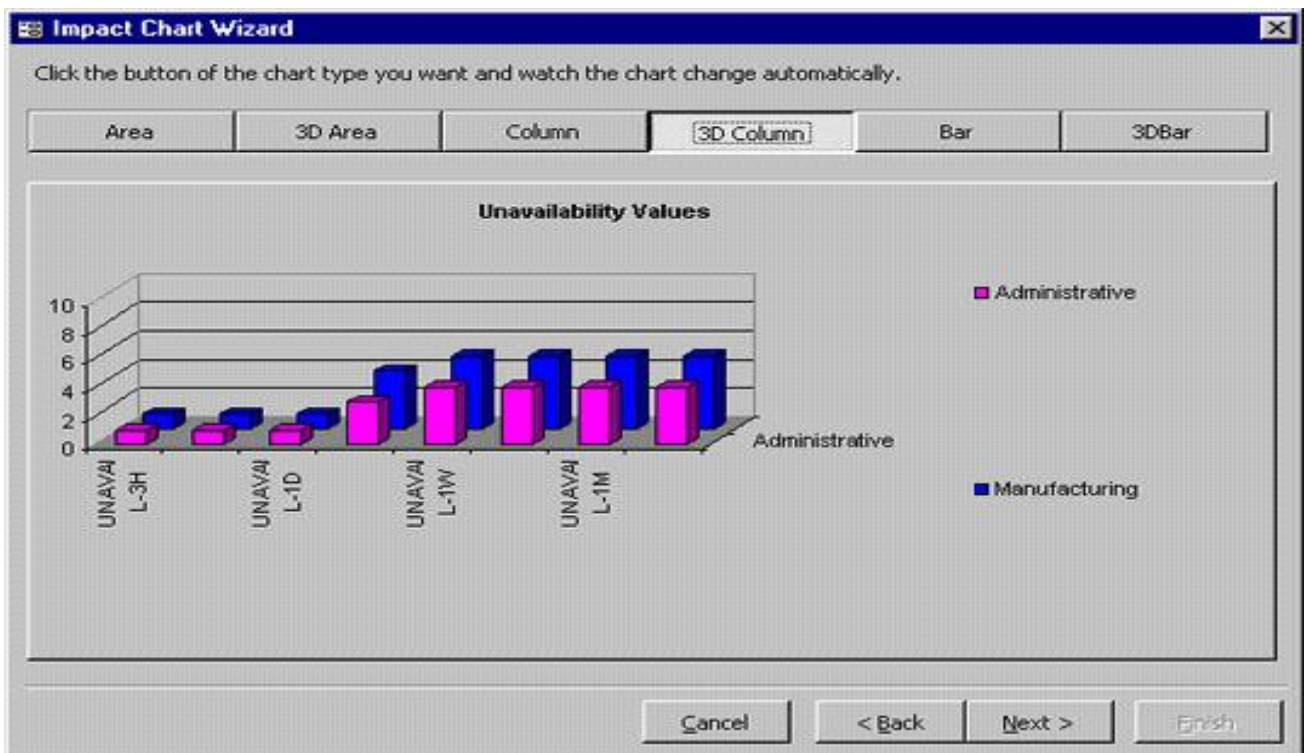


Рисунок 11 – Пример сводной оценки рисков недоступности двух информационных подсистем

- разработка мероприятий по противодействию угрозам (Рисунок 12);
- совершенствование системы реагирования на инциденты;
- устранение несоответствий требованиям стандарта ISO 17799 и других нормативных документов (Рисунок 13).



Рисунок 12 – Дерево контрмер системы CRAMM

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

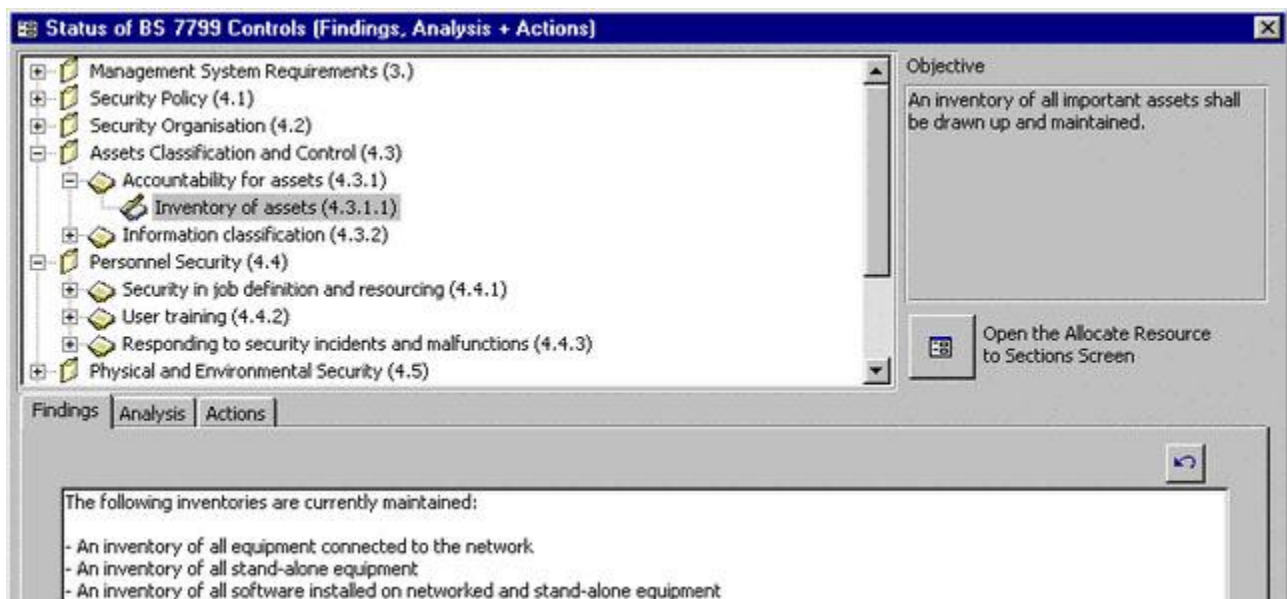


Рисунок 13 – Окно анализа несоответствий требованиям стандарта ISO17799/BS7799

Таким образом, в результате использования всех перечисленных инструментов системы CRAMM предприятие может осуществить комплекс работ по управлению информационной безопасностью и создать не только хорошо контролируемую систему защиты информации, но и информационную базу, позволяющую в будущем оценить целесообразность вложений в реализацию дополнительных мероприятий по обеспечению информационной безопасности и инвестиций в отдельные средства защиты информации.

4 Программные средства, интегрируемые в информационную систему предприятия

Еще одним направлением развития программных средств, обеспечивающих поддержку организационной работы в сфере информационной безопасности, является создание и внедрение комплексных средств анализа поведения пользователей в информационной системе. Во многом такие функции и используемые алгоритмы схожи с функциями и алгоритмами средств обнаружения вторжений. Основные функции таких программных средств:

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

- проверка действий пользователей на их соответствие действующим политикам безопасности;
- выявление нарушений действующей политики информационной безопасности;
- установление лиц, чьи действия приводят к нарушениям и создают угрозы информационной безопасности.

Основными функциями, реализуемыми программным обеспечением такого типа, являются сбор первичных данных о действиях пользователей, их автоматизированный анализ с учетом требований политики безопасности и осуществление необходимых активных действий: информирование администраторов, временное ограничение прав пользователей и пр.

Один из программных продуктов такого типа – «INSIDER – Система обнаружения внутреннего нарушителя», поставляемая российской компанией «Праймтек». Эта система накапливает сведения о поведении пользователей, а также позволяет инициировать определенные активные действия (например, для предотвращения выявленного длящегося нарушения).

В частности, для анализа поведения пользователей в информационной системе могут быть использованы следующие данные:

- показатели интенсивности использования различных пользовательских приложений;
- показатели интенсивности (частоты, объема) чтения, копирования и удаления файлов;
- показатели интенсивности отправки и приема электронных сообщений;
- показатели интенсивности передачи данных по сети;
- попытки подбора паролей;
- действия с системными файлами и реестром;
- действия с системными утилитами и пр.

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

Таким образом, у администраторов информационных систем, специалистов по информационной безопасности и руководителей предприятия появляются возможности для реагирования на инциденты, пресечения потенциально опасных действий и выявления нарушителей из числа персонала предприятия.

Также среди информационных платформ, интегрируемых в информационную систему предприятия и специально предназначенных для реализации и контроля выполнения политик безопасности, выделяются такие продукты, как:

- 1) Tivoli Security Information and Event Manager компании IBM, а также комплекс смежных продуктов, относящихся к т.н. IBM security framework
- 2) MARS: Security Monitoring, Analysis, and Response System компании Cisco.

Tivoli Security Information and Event Manager включает в себя:

- A) Tivoli Security Operations Manager.
- Б) Tivoli Compliance Insight Manager.

Tivoli Compliance Insight Manager представляет собой специальную программную платформу, которая обеспечивает контроль выполнения требований политики безопасности, а также автоматизирует значительную часть работы при проведении аудитов информационной безопасности и анализе защищенности данных. В частности, данное ПО обеспечивает сбор, анализ и защищенное хранение журналов (логов) работы различных приложений, операционных систем и платформ и их интерпретацию в терминах, понятных нетехническим специалистам. Таким образом, отчеты, формируемые данной системой, могут быть понятны бизнес-менеджерам и аудиторам и использованы для контроля выполнения требований политик безопасности.

Tivoli Security Operations Manager предназначен для контроля событий в корпоративной информационной системе и выявления нарушений и подозрительных действий в режиме близком к режиму реального времени.

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

Система MARS также обеспечивает сбор и централизованное хранение данных о системных событиях, которые поступают от различных устройств и платформ, входящих в корпоративную информационную систему, и обеспечивает возможность централизованного оперативного контроля за соблюдением установленных требований. Также MARS интегрирован с программным комплексом Cisco Security Manager, который, в свою очередь, позволяет централизованно и унифицированно управлять настройками безопасности в различных системах защиты и системах обнаружения вторжений, установленных в компании.

1 Рынок услуг по управлению информационной безопасностью

Развитие современных информационных технологий, рост зависимости деятельности многих предприятий и учреждений от функционирования информационных систем и постоянное нарастание объемов и сложности информационных потоков привели к тому, что задачи обеспечения информационной безопасности стали требовать использования значительных ресурсов. В частности, финансовые средства, выделяемые на обеспечение информационной безопасности, занимают все большую долю в бюджетах предприятий, а текущее и стратегическое управление защитой информации требует большего внимания не только со стороны специалистов по информационным технологиям, но и со стороны руководителей и собственников предприятий. Зачастую необходимые ресурсы и усилия руководителей в этой сфере оказываются сопоставимыми с теми ресурсами, которые тратятся на осуществление основной деятельности предприятий. Таким образом, сложились предпосылки для формирования рынка различных услуг по обеспечению информационной безопасности, которые (услуги) помогли бы не только повысить эффективность защиты информационных ресурсов, но и оптимизировать издержки предприятий и организаций. Основными факторами, которые обусловили появление у предприятий потребностей в услугах сторонних предприятий, решающих задачи обеспечения информационной безопасности, и выделение услуг по защите информационных ресурсов в самостоятельную сферу бизнеса, стали:

- усложнение и постоянное развитие современных систем обработки, хранения и передачи информации;
- усложнение программных и аппаратных средств, используемых для защиты информации, необходимость понимания сложного комплекса теоретических и методических вопросов для их эффективной эксплуатации;
- рост числа инцидентов и разнообразия видов атак на информационные системы и их интенсивности;

Тема 2.9 – Планирование и управление информационной безопасностью в условиях рынка
(Планирование и управление информационной безопасностью)

- нехватка квалифицированных специалистов в сфере информационной безопасности и рост затрат на их содержание и профессиональную подготовку.

- Причиной того, что предприятия оказываются заинтересованными в отказе от самостоятельного выполнения определенных функций и привлечения сторонних специализированных компаний для решения этих задач (в современной практике такой подход принято называть «аутсорсингом» или «передачей на аутсорсинг»), является возможность повысить эффективность процессов защиты информации, в определенной мере сократить издержки на эти процессы, а также в большей степени сконцентрироваться на управлении основной деятельностью предприятия и не отвлекать ресурсы и время руководителей на решение задач, являющихся по своей сути вторичными и вспомогательными по отношению к основным целям и задачам деятельности предприятия. Более высокая эффективность работы специализированных компаний – поставщиков услуг в сфере информационной безопасности по сравнению с самостоятельным решением этих задач самими предприятиями, как правило, связана с тем, что высокие издержки распределяются между множеством предприятий – клиентов поставщика услуг. Характерными примерами таких расходов, которые, с одной стороны, могут оказаться непозволительными для одного предприятия, но, с другой стороны, могут быть эффективно распределены между несколькими предприятиями, являются:

- найм высококвалифицированных специалистов в относительно узких дисциплинах и областях информационной безопасности (таких как использование криптографических средств, борьба с вирусами, внедрение виртуальных частных сетей и пр.);

- частое переобучение и повышение квалификации специалистов;

- постоянное отслеживание новых угроз и глубокий качественный анализ текущего состояния информационных технологий и тенденций их развития;

- приобретение специализированных программных и аппаратных средств, необходимых для защиты информации и аудита информационных систем;
- обеспечение круглосуточного дежурства служб реагирования на инциденты.

При всех преимуществах передачи отдельных задач обеспечения безопасности на аутсорсинг этот подход имеет и ряд недостатков, которые в определенной мере могут ограничивать его применение:

1) Предприятие, которое пользуется такими услугами, несколько ограничивает себя в возможностях управлять своими затратами и сокращать издержки (накладные расходы) и, таким образом, попадает в определенную зависимость от ценовой политики поставщиков услуг, а также от складывающейся конъюнктуры рынка.

2) Сотрудники компании, предоставляющей услуги, получают доступ к наиболее важной информации предприятия-клиента и его информационным системам, что потенциально может быть источником дополнительных рисков для информационной безопасности.

3) Возникают дополнительные угрозы информационной безопасности при взаимодействии между компанией-поставщиком и предприятием-клиентом в процессе оказания услуг (например, может быть перехвачена информация при удаленном администрировании информационных систем предприятия-клиента).

Основными услугами, которые могут быть переданы на аутсорсинг (как по отдельности, так и в комплексе), являются:

- услуги по проведению комплексных аудитов состояния информационной безопасности на предприятии;
- услуги по проведению аудитов (инструментальных проверок) устойчивости и надежности отдельных информационных подсистем (сетей,

программных и аппаратных платформ и пр.) и средств защиты информации, используемых предприятием;

- услуги по сертификации информационных систем, производимых программных и аппаратных средств защиты информации;

- консультационные услуги, связанные с формированием стратегии предприятия в сфере информационной безопасности и разработкой политики безопасности;

- услуги по проектированию системы защиты информации;

- консультационные услуги по выбору и адаптации отдельных технологий защиты информации (криптографии, биометрической идентификации и пр.) применительно к определенным условиям ведения бизнеса;

- услуги по внедрению системы защиты информации, а также внедрению отдельных технических (программных и аппаратных) средств и реализации организационных мероприятий;

- услуги по текущему администрированию, поддержке и сопровождению информационных систем и систем защиты информации;

- услуги по реагированию на инциденты, связанные с нарушениями информационной безопасности;

- услуги по обучению руководителей предприятия, специалистов службы информационной безопасности и ИТ-службы, а также пользователей информационной системы предприятия.

Также в конце этой главы мы рассмотрим еще два вида услуг, связанных с обеспечением информационной безопасности: услуги по страхованию информационных рисков и услуги по поддержанию инфраструктуры публичных ключей (Public Key Infrastructure, PKI).

В целом, к настоящему моменту сложно говорить о формировании полноценного рынка услуг в сфере информационной безопасности (особенно в России), так как у большинства менеджеров крупных, а особенно средних и

малых предприятий в основном не сформировались представления о необходимых мерах в этой сфере, а финансирование работ по обеспечению информационной безопасности зачастую осуществляется по остаточному принципу. Некоторые крупные российские разработчики комплексных решений в сфере информационной безопасности, хотя и функционируют достаточно активно, но при этом фактически не являются участниками открытого рынка, так как их продукция и услуги практически полностью ориентированы на определенных потребителей в государственном секторе, таких как ФСБ, Минатом и другие. Еще одной важной особенностью рынка услуг в сфере информационной безопасности является то, что оказание таких услуг иногда становится «побочным», дополнительным видом (направлением) деятельности для компаний, занимающихся поставкой аппаратных и программных средств защиты информации (так называемых «коробочных продуктов»), а также для компаний, занимающихся разработкой комплексных решений по автоматизации предприятий. Возможным недостатком такого подхода потенциально может быть то, что консультанты и аналитики оказываются жестко «привязаны» к определенным программным и аппаратным средствам (производителям, торговым маркам) и не имеют возможности гибко подбирать отдельные средства защиты и формировать наиболее эффективные комплексные решения в соответствии с потребностями каждого конкретного предприятия.

Тем не менее, несмотря на определенные недостатки в развитии рынка услуг по обеспечению информационной безопасности, неоспоримым фактом является то, что многие такие услуги уже представлены на рынке, а основные рыночные и организационные механизмы начинают отрабатываться на практике. При этом одной из рекомендаций при работе с предприятиями-поставщиками услуг в сфере информационной безопасности является правило - пользоваться услугами нескольких разных предприятий и периодически менять партнеров, обеспечивающих решение тех или иных проблем безопасности.

2 Характеристики услуг управления информационной безопасностью

Каждый вид услуг в этой сфере имеет свои специфические характеристики как с точки зрения организации работы компаний, оказывающих услуги, так и с точки зрения структуры рынка. Соответственно, для эффективной работы необходим индивидуальный подход к организации оказания таких услуг, а также организации взаимодействия между потребителями и поставщиками услуг.

1) Услуги по реагированию на инциденты (нарушения информационной безопасности), уже частично рассмотренные в одном из предыдущих разделов, являются одним из наиболее характерных примеров обоснованности и целесообразности передачи сервисов безопасности на аутсорсинг. В частности, целесообразность отказа от самостоятельного выполнения функций реагирования на инциденты и их (функций) централизации в специализирующейся на таких задачах компании связана с тем, что эта деятельность имеет следующие важные особенности:

- требует постоянного (круглосуточного) дежурства, что предполагает содержание в штате как минимум пяти специалистов;
- предполагает наличие высококвалифицированных (а следовательно, высокооплачиваемых и востребованных на рынке труда) специалистов, способных быстро предпринять эффективные меры противодействия возникающим угрозам (в том числе и применить контрмеры к нападающим в процессе длящейся атаки), а также самостоятельно принять необходимые решения в процессе отражения длящейся атаки;
- загрузка дежурных специалистов, отвечающих за реагирование на инциденты, может быть крайне неравномерной.

Таким образом, эффект от централизации функций, связанных с реагированием на инциденты, складывается из нескольких составляющих и предоставляет возможности как для сокращения затрат и повышения уровня

защищенности предприятий-клиентов, так и для получения прибыли предприятиями-поставщиками таких услуг.

При этом разграничение функций между предприятием-клиентом и компанией-поставщиком услуг может зависеть от таких факторов, как:

- уровень доверия предприятия-клиента к предприятию-поставщику услуг;
- сложившаяся практика оказания таких услуг и наличие у предприятий-поставщика необходимых специалистов с определенным уровнем квалификации;
- состав, характеристики и функциональность информационных систем предприятия-клиента;
- уровень квалификации сотрудников предприятия-клиента (как пользователей информационных систем, так и сотрудников департамента информационной безопасности);
- оценка существующих рисков (вероятности нанесения ущерба);
- оценка (в том числе и субъективная) того, насколько значимым является знание внутренней среды предприятия сотрудниками службы информационной безопасности и их способность «изнутри» координировать действия и решать проблемы в случае каких-либо инцидентов.

Кроме того, в некоторых случаях могут существовать определенные законодательные ограничения на аутсорсинг процессов безопасности (в частности, для государственных предприятий).

2) Основные вопросы проведения аудитов информационной безопасности (и, в частности, внешних аудитов) уже рассматривались нами в предыдущей лекции. Помимо уже указанных факторов, которые обуславливают необходимость проведения именно внешних аудитов, а не внутренних (более высокая квалификация специалистов, право делать заключения о соответствии международным стандартам и пр.), важным является также и то обстоятельство, что внешние аудиторы, как правило, не заинтересованы в

представлении необъективной информации (в отличие от внутренней службы информационной безопасности). В случае же, если предприятие захочет создать собственную независимую службу для проведения аудитов информационной безопасности (отдельно от департамента информационной безопасности и других подразделений предприятия), результатом могут оказаться очень большие затраты, тем более что частота проведения таких аудитов, как правило, является не очень большой.

3) Необходимость прибегать к услугам специализированных предприятий, связанным с проверкой защищенности и надежности отдельных элементов информационной инфраструктуры (серверов, сетей, межсетевых экранов и пр.), обусловлена, как правило, наличием у этих предприятий специализированных программных и аппаратных средств, необходимых для проведения таких проверок (например, специализированных сканеров уязвимостей), а также наличие специальных знаний и навыков и разностороннего опыта, накопленного в процессе практической работы при проведении подобных проверок на различных предприятиях. Приобретение подобного опыта в рамках одного предприятия, пусть даже и очень крупного, практически невозможно.

Одним из наиболее эффективных приемов при проведении такого рода проверок является пробное (тестовое) преодоление защиты, когда проверяющий имитирует определенное нападение с целью совершить нарушение (разрушить базу данных, выкрасть конфиденциальную информацию и пр.). Основными задачами проверок такого рода являются:

- оценка эффективности используемых технических (программных и аппаратных) средств защиты информации;
- оценка эффективности работы специалистов, ответственных за реагирование на инциденты;
- контроль соблюдения сотрудниками предприятия требований политики безопасности.

Для получения наиболее достоверных результатов желательно, чтобы на самом предприятии о проведении такого теста знали только несколько руководителей, ответственных за его организацию. Также важным условием проведения такой проверки является четкая договоренность о том, насколько далеко должна зайти атака и какой уровень проникновения и разрушительных действий является достаточным, для того чтобы достоверно продемонстрировать, что атакуемая (проверяемая) система является уязвимой. В любом случае вся ответственность за ущерб, нанесенный в результате осуществления такой проверки, полностью ложится на предприятие, заказавшее такую услугу.

3) Консультационные услуги, связанные с первичной постановкой системы управления информационной безопасностью (первичным анализом, формированием и внедрением политики безопасности), обычно бывают необходимы в той ситуации, когда предприятие впервые ставит для себя задачу целенаправленного систематического комплексного обеспечения информационной безопасности. В этих условиях привлечение сторонних консультантов является практически единственным способом сформировать достаточно адекватную и эффективную политику безопасности в относительно короткие сроки, так как само предприятие в такой ситуации обычно не имеет необходимых специалистов и руководителей, которые могли бы решить весь комплекс задач, связанных с оценкой рисков, инвентаризацией информационных активов, выработкой стратегии, формированием политики и организационной структуры департамента информационной безопасности.

Привлекаемая для решения всех этих задач консультационная компания должна будет провести анализ деятельности предприятия в нескольких разрезах: с точки зрения основных бизнес-процессов, с точки зрения имеющейся информационно-технологической и коммуникационной инфраструктуры, а также с точки зрения используемых приложений (программного обеспечения и баз данных). Таким образом, необходимое качество работы по обеспечению комплексной защищенности

информационных ресурсов предприятия может быть достигнуто только в том случае, если у консалтинговой компании имеются необходимые специалисты, а также опыт работы как на подобных предприятиях, так и с подобными программными и аппаратными платформами. Высокие требования к квалификации специалистов, работающих в консалтинговых компаниях, объясняются необходимостью не просто понять особенности функционирования тех или иных бизнес-процессов и информационных систем, но и достаточно быстро оценить их слабые места, существующие риски и наиболее вероятные сценарии нанесения ущерба информационным ресурсам.

4) Услуги по администрированию информационных систем и средств защиты информации могут предоставляться как в комплексе с услугами по реагированию на инциденты, так и независимо от них. Предприятия-поставщики услуг могут осуществлять администрирование таких систем, как:

- электронная почта (защита от вирусов, спама, нарушения конфиденциальности и других нарушений политики безопасности);
- сетевое оборудование (сбор и анализ информации о функционировании маршрутизаторов, серверов и других устройств);
- брандмауэры (конфигурирование и настройка доступа к сети, а также обеспечение своевременного реагирования на различные нарушения);
- системы обнаружения вторжений (отслеживание всех «подозрительных» действий в отношении сетей, серверов, приложений и баз данных).

При этом предприятие-клиент может прибегать к услугам других предприятий для контроля за тем, насколько эффективно осуществляется администрирование средств защиты информации, либо самостоятельно осуществлять такой контроль при помощи специальных сканеров.

При оказании услуг по администрированию предприятий-поставщик, как правило, не может взять на себя полную ответственность за сохранность информации (так же как и при оказании услуг по реагированию на инциденты),

однако для установления формальных отношений предприятие-клиент и предприятия-поставщик могут выработать Соглашение об уровне обслуживания, которое должно предусматривать основные параметры функционирования информационных систем и их защищенности (гарантированное время надежной работы систем, гарантированные сроки восстановления работоспособности при нарушениях и пр.).

3 Инфраструктура публичных ключей

Инфраструктура публичных ключей (Public Key Infrastructure, PKI) представляет собой сложную организационно-техническую систему, основанную на современных технологиях и развитых организационных стандартах, которая позволяет эффективно решать некоторые ключевые проблемы информационной безопасности и, в частности, проблемы защиты данных, передаваемых по сетям (как локальным, так и глобальным), и идентификации сторон, участвующих в информационном обмене (пользователей, информационных систем, программных процессов). Технология PKI является основным инструментом, при помощи которого на основе законодательной базы (в частности, на основе Федерального Закона РФ «Об электронной цифровой подписи», принятого в 2002 году) может быть создан юридически значимый документооборот, который, в свою очередь, может стать основой для активного развития электронной торговли, оказания финансовых, информационных и других услуг, а также осуществления электронных платежей через информационные сети общего пользования. Возможность использования этой технологии для осуществления платежей и хозяйственных сделок связана с тем, что ее самым важным элементом является так называемый цифровой сертификат, выдаваемый третьей стороной, которая фактически является гарантом того, что сделки, совершаемые с использованием определенного цифрового сертификата, совершаются от имени определенного лица. Таким образом, одним из ключевых элементов инфраструктуры публичных ключей являются так называемые «удостоверяющие центры»² (Certificate Authority, CA) – организационные структуры, осуществляющие

идентификацию личностей (если речь идет о выдаче сертификата для одного человека) и выдачу электронного сертификата установленного образца, однозначно и достоверно представляющего этого человека. Также эти центры решают множество дополнительных задач, связанных с обеспечением эффективной работы инфраструктуры публичных ключей: ведут списки аннулированных сертификатов, обновляют истекшие сертификаты и пр. В целом вся совокупность используемых технических и организационных решений, а также действующая юридическая база дают возможность однозначно связывать цифровой сертификат (цифровую подпись) с определенным физическим лицом и также гарантировать, что не происходит нарушения целостности передаваемых сообщений.

В настоящее время достаточно хорошо разработаны базовые технические стандарты и информационные технологии (средства криптографии, алгоритмы, реализующие хэш-функции и пр.), необходимые для построения средств защиты на основе PKI. Дальнейшие перспективы развития в данной сфере связаны, главным образом, с совершенствованием рынка услуг и организационных механизмов.

Идеология работы PKI предполагает создание сетей и иерархически взаимосвязанных структур множества различных удостоверяющих центров, работающих в рамках единой согласованной политики и опирающихся на общий «корневой» удостоверяющий центр. На практике же наиболее распространено создание самостоятельных разрозненных удостоверяющих центров, создаваемых отдельными предприятиями (например, коммерческими банками) на основе тиражируемых программных и аппаратных решений для обеспечения защищенности и придания юридической значимости создаваемым документам и транзакциям, осуществляемым в корпоративных информационных системах (таким как, например, платежные поручения) служащими, клиентами и бизнес-партнерами предприятия. В случае если предприятие самостоятельно развертывает PKI в рамках собственной информационной системы, все взаимоотношения между администрацией и

пользователями регулируются внутренней политикой, вопросы разработки которой были рассмотрены в предыдущей главе.

При этом одним из возможных подходов к внедрению технологии РКІ является передача функций, связанных с выдачей и дальнейшим обращением цифровых сертификатов, на аутсорсинг. Передача функций удостоверяющего центра сторонней специализированной компании, как правило, решает для предприятия две важных задачи:

- позволяет избежать значительных расходов, связанных с закупкой и поддержанием программных и аппаратных средств, а также наймом и обучением персонала;
- дает возможность применять цифровые сертификаты за пределами своего предприятия, а также использовать на предприятии сертификаты сотрудников других предприятий.

В свою очередь, компания, выполняющая функции удостоверяющего центра, может передать часть работ, которые связаны с проверкой документов лиц, претендующих на получение сертификата, и их консультированием, своим партнерам – так называемым «регистрационным центрам». Их основная функция заключается в упрощении и ускорении процедуры проверки документов и идентификации личности при выдаче сертификата для лиц, которые не могут лично явиться в удостоверяющий центр.

Именно на основе сетей регистрационных центров, а также взаимодействия различных удостоверяющих центров (их объединения в единую сеть) должно происходить построение универсальной общедоступной инфраструктуры публичных ключей. Предполагается, что основными пользователями – клиентами удостоверяющих центров, желающими получить цифровые сертификаты, – должны быть лица, заинтересованные в доступе к различным специализированным электронным сервисам, облегчающим взаимодействие как с различными коммерческими структурами (например, банками), так и с государственными органами. Однако на практике

продвижение технологии РКІ и ее широкое использование сильно затруднено в связи с множеством объективных и субъективных факторов, таких как:

- неготовность многих предприятий и особенно государственных органов к использованию данной технологии и, в частности, к параллельному использованию как обычных «бумажных» документов, так и электронных (заверенных электронными подписями);
- отсутствием у многих людей достаточных навыков обращения с компьютерной техникой, а также доступа в сеть Интернет;
- отсутствием у многих людей культуры использования электронных документов и электронной подписи, за которую необходимо нести ответственность;
- ограниченная совместимость некоторых средств защиты информации, используемых в России, со средствами защиты информации, применяемыми в других странах.

В результате перспективы решения важных организационных задач, таких как унификация технологий электронно-цифровой подписи и развитие общефедеральных удостоверяющих центров, оказываются неопределенными и во многом зависят от квалификации отдельных представителей профессионального сообщества и их отношения к данной проблеме.

1 Основы методологии страхования информационных рисков

Хотя страхование рисков, связанных с информационной безопасностью, само по себе не является организационным средством защиты информации (так как факт наличия или отсутствия такой страховки не влияет на вероятность нанесения ущерба информационным ресурсам), все же оно является важным и перспективным инструментом управления информационными рисками на предприятии. С точки зрения риск-менеджмента, страхование является главным инструментом так называемой «передачи рисков». Основным фактором, обуславливающим заинтересованность предприятий в страховании своих информационных ресурсов, является то, что в случае каких-либо серьезных нарушений в работе информационных систем предприятие получает возможность за счет страховых выплат относительно быстро восстановить их (систем) работу, а также основные бизнес-процессы и компенсировать (хотя бы частично) ущерб от вынужденного простоя и потери информационных активов.

Согласно Закону РФ «Об организации страхового дела в Российской Федерации», объектом страхования могут быть не противоречащие законодательству имущественные интересы, связанные с владением, пользованием, распоряжением имуществом, а также связанные с возмещением страхователем причиненного им вреда личности или имуществу физического лица, а также вреда, причиненного юридическому лицу (страхование ответственности). Таким образом, на практике объектами страхования могут быть:

- информационные ресурсы (в любом их виде: базы данных, библиотеки электронных документов и пр.);
- программное обеспечение (как уже используемые программные собственные и покупные продукты, так и находящиеся в разработке);
- аппаратное обеспечение информационных систем (сетевое оборудование, серверы, рабочие станции, телекоммуникационное оборудование, периферия, источники бесперебойного питания и пр.);

Тема 2.10 – Страхование информационных рисков
(Планирование и управление информационной безопасностью)

– финансовые активы (денежные средства, бездокументарные ценные бумаги) в электронной форме (в том числе средства на счетах, управляемых при помощи систем «клиент-банк»).

Договор страхования (страховой полис) может предусматривать возмещение прямых убытков в случае наступления различных страховых случаев, таких как:

– выход из строя (сбои в работе) информационных систем, обусловленные недостаточным качеством используемых программных и аппаратных средств, ошибками при их проектировании, разработке, производстве, установке, настройке, обслуживании или эксплуатации;

– умышленные противоправные действия сотрудников предприятия, совершенные с целью нанести ущерб предприятию либо получить определенную выгоду;

– нападения (атаки) на информационные системы предприятия, которые совершены третьими лицами с целью нанести ущерб информационным ресурсам предприятия и его информационным системам (повредить или уничтожить информацию, хранящуюся в электронном виде, получить конфиденциальные сведения, вывести из строя программные и аппаратные средства с целью прекратить или приостановить функционирование определенных сервисов и пр.);

– воздействия вредоносных программ и макросов (вирусов, червей и пр.), повлекшие нарушения работы информационных систем, потерю информации или разглашение конфиденциальной информации;

– хищение финансовых активов (денежных средств, бездокументарных ценных бумаг), совершенное путем осуществления различных неправомерных действий: кражи паролей и ключей, присвоения личности, внесения изменений в программное обеспечение и пр.

В дополнение к основным рискам, непосредственно связанным с информационными активами, также могут быть застрахованы:

- убытки от приостановки основной хозяйственной деятельности предприятия в результате нарушения работы информационных систем;
- дополнительные расходы, связанные с поддержанием текущей хозяйственной деятельности в период восстановления работы поврежденных информационных систем;
- дополнительные расходы, связанные со срочным восстановлением работы информационных систем, а также срочным восстановлением основной хозяйственной деятельности предприятия;
- дополнительные расходы на восстановление деловой репутации после того, как ей был нанесен ущерб в результате атаки на информационные ресурсы и информационные системы (Public Relations Coverage).

Убытки от приостановки основной хозяйственной деятельности предприятия могут включать в себя упущенную выгоду, обусловленную простоем информационных систем (т.е. ту прибыль, которую предприятие могло бы получить, но не получило по причине выхода из строя информационных систем), а также расходы по поддержанию инфраструктуры предприятия в период вынужденного простоя (как правило, это некоторые постоянные расходы, не зависящие от объема выпуска продукции и интенсивности хозяйственной деятельности). Дополнительные расходы, связанные с поддержанием текущей хозяйственной деятельности в период восстановления работы поврежденных информационных систем, могут возникать в том случае, если существуют некоторые альтернативные способы обработки и хранения информации и осуществления бизнес-процессов (например, на базе программных и аппаратных средств, а также телекоммуникационных каналов, временно арендуемых у специализированных компаний) и предприятие сочтет нужным и возможным воспользоваться этими альтернативными способами. При этом задействование таких резервных ресурсов, как правило, должно быть согласовано со страховой компанией, покрывающей эти расходы. Дополнительные расходы, связанные со срочным

восстановлением работы информационных систем, могут возникать в том случае если, например, у сторонних поставщиков существуют некоторые альтернативные (более оперативные по сравнению с обычными) условия поставок оборудования и программного обеспечения, а также предоставления услуг по вводу в действие информационных систем.

Все эти расходы, очевидно, также могут быть объектами страхования. При этом в каждой ситуации страховщику и страхователю необходимо детально проанализировать различные альтернативы выхода из кризисной ситуации и выбирать наиболее целесообразные варианты. Так, например, страховая компания может отказаться компенсировать дополнительные издержки, связанные со срочным восстановлением информационных систем, если более выгодной является компенсация упущенной выгоды за период более длительного вынужденного простоя.

Процедура страхования (жизненный цикл договора страхования) включает в себя несколько основных этапов (Рисунок 1).

- 1) Предварительное обследование предприятия, анализ существующих рисков для информационной безопасности.
- 2) Формулирование рекомендаций по уменьшению рисков и реализация предприятием соответствующих мероприятий.
- 3) Согласование условий страхования и заключение договора.
- 4) Анализ ущерба и его расчет в денежном выражении в случае реализации застрахованных рисков.
- 5) Согласование и последующее осуществление страховых выплат, покрывающих ущерб.

Тема 2.10 – Страхование информационных рисков
(Планирование и управление информационной безопасностью)

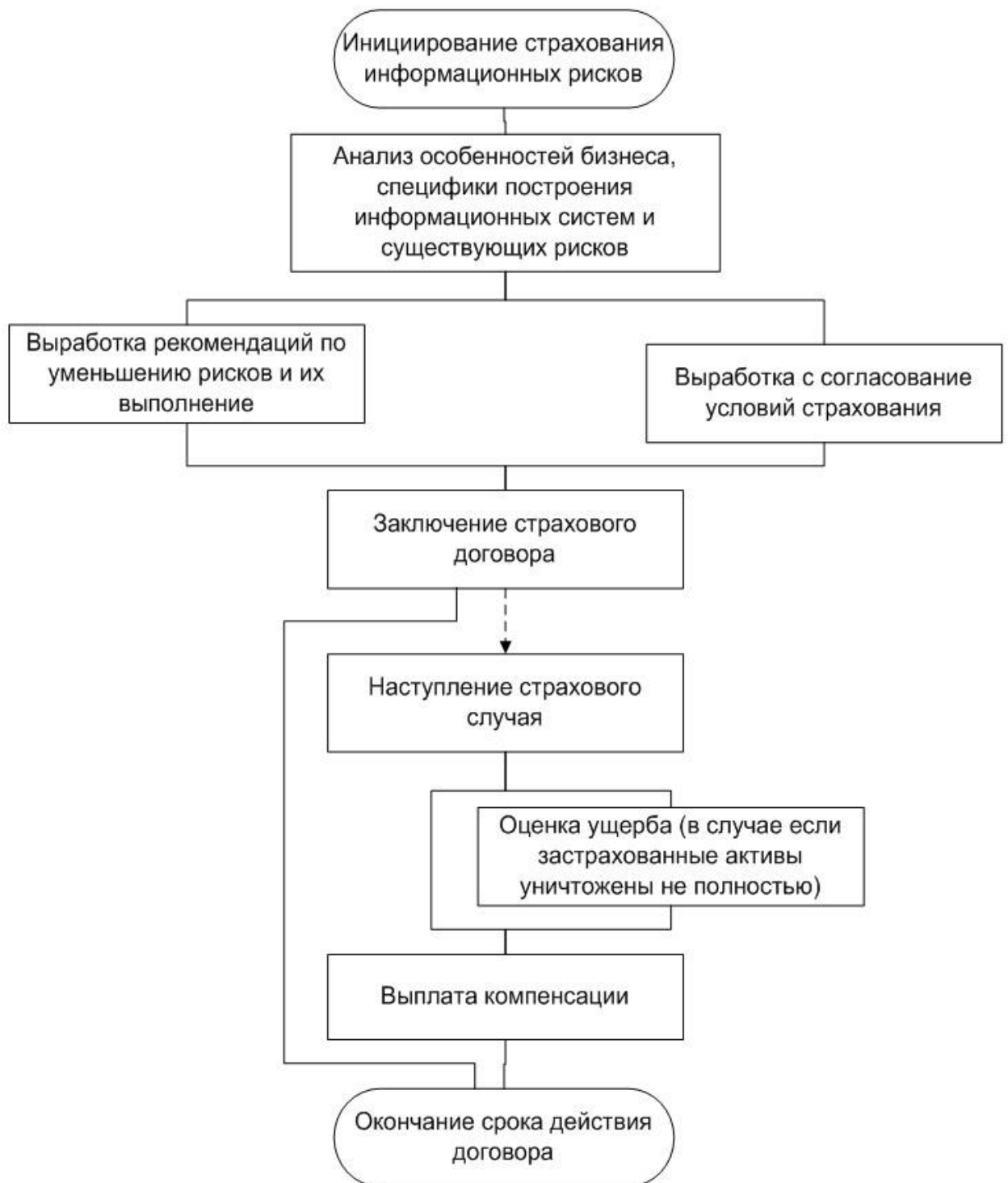


Рисунок 1 – стадии процесса страхования информационных рисков

Предварительное обследование предприятия до заключения договора страхования во многом аналогично проведению внешнего аудита и также может осуществляться независимой специализированной компанией. По окончании такой проверки могут быть сформированы два основных документа:

- отчет (заключение) о состоянии информационной безопасности на предприятии;
- рекомендации по повышению уровня защищенности информационных ресурсов и уменьшению рисков.

Такое обследование в дальнейшем создает предпосылки для принятия решения о возможности и целесообразности страхования информационных рисков данного предприятия, а также для обоснованного количественного анализа рисков и определения основных параметров договора страхования.

На основе оценок рисков (с учетом реализации рекомендованных мероприятий по их уменьшению) определяется одно из наиболее существенных условий договора страхования – ставка страхования. Как правило, ее размер не превышает пяти процентов, однако на практике он может варьироваться в диапазоне от нескольких десятых долей процента до пяти и более процентов. На размер ставки в каждом конкретном случае могут повлиять несколько факторов:

- статистические данные, касающиеся нарушений информационной безопасности на аналогичных предприятиях (в сопоставимых условиях);
- уровень защищенности информационных ресурсов данного предприятия (качество используемых технических средств, уровень организационного обеспечения информационной безопасности на предприятии и пр.);
- интенсивность текущей хозяйственной деятельности (выполнения текущих бизнес-операций);

– страховая сумма – стоимость информационных активов, подлежащих страхованию (как правило, чем больше стоимость страхуемых ресурсов, тем ниже удельная ставка страхования).

Помимо ставки страхования в процессе согласования условий договора также определяется другой важный параметр – лимит ответственности страховой компании (максимальная величина средств, которые могут быть выплачены страховщиком страхователю в течение всего срока действия договора страхования). Как правило, страховая сумма должна быть достаточно большой, чтобы у страховой компании была возможность компенсировать накладные расходы (в частности, расходы на предварительное обследование предприятия), связанные с заключением договора страхования.

В случае реализации риска (возникновения страхового случая) застрахованные информационные ресурсы могут быть полностью утрачены. При этом страховая компания должна будет произвести страховые выплаты в полном объеме (в пределах установленного лимита ответственности). В случае, если повреждена только часть информационных ресурсов, для предприятия и страховой компании начинается сложный процесс определения суммы ущерба, которая должна быть компенсирована. Такая оценка также может быть произведена независимой третьей стороной. Кроме того, предметом анализа в этой ситуации могут быть все обстоятельства, связанные с произошедшим страховым случаем. В частности, договором страхования может быть предусмотрена обязанность предприятия-клиента предпринять ряд мер в рамках определенного плана аварийных мероприятий с целью минимизировать ущерб. Таким образом, страховая компания, прежде чем произвести выплаты, должна будет убедиться в том, что предприятием-клиентом были предприняты определенные меры предосторожности.

То обстоятельство, что взаимодействие страховщика и страхователя при определении размера страховых выплат является одним из наиболее проблемных вопросов, заставляет передовые компании искать новые формы организации процесса страхования. Так, например, для разрешения проблем

при реализации некоторых страховых рисков и уменьшения убытков третьей стороной в договоре страхования может выступать компания – поставщик информационных систем и комплексных решений, которая при наступлении страхового случая может на некоторое время (на период восстановительных работ) предоставить резервные программные и аппаратные средства для обеспечения непрерывности основной деятельности предприятия-страхователя, а также организовать сами восстановительные работы. В этом случае страховая компания может сократить размер страховых выплат на компенсацию упущенной выгоды предприятия-страхователя и избежать некоторых излишних выплат на восстановление утраченных информационных ресурсов.

Помимо страхования собственно информационных рисков, также важное значение имеет страхование гражданской ответственности компаний, оказывающих информационные услуги и услуги по защите информации большому числу пользователей:

- страхование гражданской ответственности удостоверяющих центров, работающих в инфраструктуре публичных ключей;
- страхование ответственности фондовых бирж и других электронных торговых площадок по возмещению имущественного вреда третьим лицам;
- страхование гражданской ответственности разработчиков и поставщиков средств защиты информации.

Необходимость страхования гражданской ответственности компаний-поставщиков продуктов и услуг перед потребителями в этом случае обусловлена тем, что их услугами (продуктами) пользуется большое число клиентов, каждый из которых с использованием этих продуктов и услуг управляет дорогостоящими информационными активами (финансовыми средствами, конфиденциальными сведениями, разглашение которых может привести к огромным убыткам, и пр.). Таким образом, у компаний-поставщиков таких продуктов и услуг возникают риски того, что к ним будут предъявлены иски о возмещении ущерба, понесенного клиентами вследствие

того, что злоумышленники воспользовались уязвимостями в поставляемых продуктах. Очевидно, что собственные активы и доступные средства, имеющиеся у компаний-поставщиков, как правило, гораздо меньше потенциально возможного ущерба, который может возникнуть у их клиентов. В результате этого страхование оказывается единственным средством обеспечения ответственности и, следовательно, построения цивилизованных взаимоотношений на рынке средств защиты информации, а также услуг по защите информации.

2 Рынок страховых услуг

Мировая практика страхования информационных рисков начала складываться в девяностых годах и получила свое развитие после 2000-го года, когда, с одной стороны, риски информационной безопасности стали более серьезными, чем когда-либо, а с другой – в западных странах окончательно сложилась практика не включать информационные риски в универсальные страховые полисы, которыми обычно покрывались основные бизнес-риски.

Таким образом, к настоящему времени крупнейшими мировыми компаниями, оказывающими услуги по страхованию информационных рисков, являются:

- Британская страховая компания «Lloyds of London»;
- американская компания «AIG»;
- Zurich North America («The E-Risk Edge solution»);
- страховая группа «Chubb»;
- страховая компания «Marsh».

Страхование информационных рисков компанией Lloyds of London осуществляется совместно с известной компанией Counterpane, предоставляющей услуги по оценке состояния защищенности информационных ресурсов и по текущей поддержке информационной безопасности. Также в этой работе участвуют компании Frank Crystal & Co. и SafeOnline Ltd. Эти предприятия предлагают два основных совместных страховых продукта:

Тема 2.10 – Страхование информационных рисков
(Планирование и управление информационной безопасностью)

- Internet Asset and Income Protection Coverage («Покрытие рисков, связанных с информационными активами и информационной деятельностью»)
- программа страхования информационных ресурсов отдельных компаний;
- Internet Asset and Income Protection Warranty Plan («План гарантирования информационных активов и информационной деятельности») – основанный на страховании план гарантирования надежности работы поставщиков услуг Интернет.

Американская страховая компания American International Group, Inc. (AIG), действующая в 130 странах мира, в лице своего подразделения AIG eBusiness Risk Solutions (AIG eBRS) предлагает программу страхования информационных рисков netAdvantage (AIG netAdvantage Suite). В рамках своей комплексной программы страхования эта компания предлагает скидки клиентам, пользующимся определенными средствами защиты информации. Для обеспечения эффективности и комплексности услуг по страхованию AIG eBRS организует технологические альянсы с компаниями, поставляющими средства защиты информации, а также проводящими аудиты безопасности.

В рамках программы netAdvantage предлагается несколько вариантов страховой защиты:

- защита от ущерба в случае неправомерного разглашения частных данных;
- защита от уничтожения (утраты) данных или программного обеспечения;
- защита от ущерба в случае нарушения операционной деятельности (упущенная выгода и дополнительные расходы) в случае нарушений информационной безопасности;
- страховая компенсация затрат на нейтрализацию уязвимостей;
- страховая компенсация затрат на восстановление деловой репутации (PR) в случае реализации рисков.

Тема 2.10 – Страхование информационных рисков
(Планирование и управление информационной безопасностью)

В России одной из первых компаний, начавших предоставлять услуги такого рода, стал «Ингосстрах». В 1999 году было подписано «Соглашение о сотрудничестве в области страхования информационных ресурсов» между Министерством РФ по связи и информатизации, с одной стороны, и страховыми компаниями «Ингосстрах» и «Инфистрах» – с другой. Начиная с 2000 года некоторые российские страховые компании получили лицензии на осуществление такой деятельности, однако в целом этот рынок в России остается неразвитым. Деятельность страховых компаний, как правило, ориентирована на страхование банковских рисков и крупных объектов (таких как «Российская торговая система», РТС или система межбанковского процессингового центра электронного документооборота Faktura.Ru), при этом некоторые сегменты этого рынка практически не развиваются.

1 Основы экономики информационной безопасности

Управление информационной безопасностью, так же, как и управление во многих других сферах деятельности, предполагает периодическое принятие различных управленческих решений, заключающихся, как правило, в выборе определенных альтернатив (отборе одной из возможных организационных схем или одного из доступных технических решений) или определении некоторых параметров отдельных организационных и/или технических систем и подсистем. Одним из возможных подходов к выбору альтернатив в ситуации принятия управленческого решения является т.н. «волевой» подход, когда решение по тем или иным причинам принимается интуитивно, и формально обоснованная причинно-следственная взаимосвязь между определенными исходными предпосылками и конкретным принятым решением не может быть установлена. Очевидно, что альтернативой «волевому» подходу становится принятие решений, основанное на определенных формальных процедурах и последовательном анализе.

Основой такого анализа и последующего принятия решений является экономический анализ, предполагающий изучение всех (или хотя бы основных) факторов, под влиянием которых происходит развитие анализируемых систем, закономерностей их поведения, динамики изменения, а также использование универсальной денежной оценки. Именно на основе адекватно построенных экономических моделей и осуществляемого с их помощью экономического анализа должны приниматься решения, касающиеся как общей стратегии развития, так и отдельных организационных и технических мероприятий, как на уровне государств, регионов и отраслей, так и на уровне отдельных предприятий, подразделений и информационных систем.

При этом, так же как и экономика любой отрасли деятельности имеет свои особенности, экономика информационной безопасности, рассматриваемая как относительно самостоятельная дисциплина, с одной стороны, базируется на некоторых общих экономических законах и методах анализа, а с другой – нуждается в индивидуальном понимании, развитии специфических подходов к

анализу, накоплении статистических данных, специфичных для этой сферы, формировании устойчивых представлений о факторах, под влиянием которых функционируют информационные системы и средства защиты информации.

Сложность задач экономического анализа практически во всех областях деятельности, как правило, обуславливается тем, что многие ключевые параметры экономических моделей невозможно достоверно оценить, и они носят вероятностный характер (такие как, например, показатели потребительского спроса). Анализ усложняется также тем, что даже небольшие колебания (корректировка оценок) таких параметров могут серьезно повлиять на значения целевой функции и, соответственно, на решения, принимаемые по результатам анализа. Таким образом, для обеспечения как можно большей достоверности расчетов в процессе проведения экономического анализа и принятия решений необходимо организовать комплекс работ по сбору исходной информации, расчету прогнозных значений, опросу экспертов в различных областях и обработке всех данных. При этом в процессе проведения такого анализа необходимо уделять особое внимание промежуточным решениям, касающимся оценок тех или иных параметров, входящих в общую модель. Необходимо также учитывать то обстоятельство, что сам по себе такой анализ может оказаться достаточно ресурсоемкой процедурой и потребовать привлечения дополнительных специалистов и сторонних консультантов, а также усилий со стороны различных специалистов (экспертов), работающих на самом предприятии, – все эти затраты, в конечном счете, должны быть оправданы.

Особая сложность экономического анализа в такой сфере, как информационная безопасность, обуславливается такими специфическими факторами, как:

- быстрое развитие информационных технологий и методик, используемых в этой сфере (как средств и методов защиты, так и средств, и методов нападения);

Тема 2.11 – Экономика планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

- невозможность достоверно предугадать все возможные сценарии нападения на информационные системы и модели поведения нападающих;

- невозможность дать достоверную, достаточно точную оценку стоимости информационных ресурсов, а также оценить последствия различных нарушений в денежном выражении.

Это требует дополнительных усилий по организации процесса экономического анализа, а также зачастую приводит к тому, что многие принимаемые решения, относящиеся к обеспечению информационной безопасности, могут оказаться неадекватными. Примерами ситуаций, в которых недостаточная развитость методологии экономического анализа негативно влияет на состояние информационной безопасности, могут быть случаи, когда:

- руководство предприятия может принять неадекватные решения относительно инвестиций в средства защиты информации, что, в свою очередь, может привести к убыткам, которых можно было избежать;

- руководство предприятия может принять определенные решения относительно организации бизнес-процессов и процессов обработки информации на предприятии, исходя из стремления сократить текущие затраты и уменьшить нагрузку на персонал, при этом не принимая во внимание экономические последствия недостаточной защищенности информационных ресурсов;

- страхователь и страховщик могут не заключить договор о страховании информационных рисков или установить неадекватные параметры такого договора ввиду того, что отсутствуют модели и методы оценки экономических параметров сделки.

2 Анализ вложений в средства защиты информации

В процессе текущей деятельности предприятиям постоянно приходится сталкиваться с теми или иными изменениями: уточняются бизнес-процессы, меняется конъюнктура рынков сбыта и рынков потребляемых материальных ресурсов и услуг, появляются новые технологии, изменяют свое поведение конкуренты и контрагенты, меняется законодательство и политика государства и т.д. В этих условиях менеджерам (в том числе и руководителям, отвечающим за обеспечение информационной безопасности) приходится постоянно анализировать происходящие изменения и адаптировать свою работу к постоянно меняющейся ситуации. Конкретные формы, в которых проявляется реакция руководителей, могут быть различными. Это может быть смена маркетинговой политики, реорганизация бизнес-процессов, изменение технологий, изменение производимого продукта, слияние с конкурентами или их поглощение и пр. Однако при всем разнообразии возможных моделей поведения в меняющейся среде почти всех их объединяет один важный общий для них методологический элемент: в большинстве случаев реакция бизнеса на новые угрозы и новые возможности предполагает осуществление новых более или менее долгосрочных и ресурсоемких вложений (инвестиций) в определенные организационные и/или технические мероприятия, которые, с одной стороны, предполагают расходование ресурсов (денежных средств), а с другой – дают возможность получить новые выгоды, выражающиеся в увеличении дохода или сокращении некоторых текущих расходов.

Таким образом, в ситуации, когда необходимо осуществить некоторые новые организационные или технические мероприятия (реализовать проект), основной задачей лиц, отвечающих за эффективную организацию информационной безопасности, является четкое соотнесение затрат, которые придется понести в связи с реализацией этого мероприятия (как единовременные, так и постоянные текущие), и дополнительных (новых) денежных потоков, которые будут получены. В данном случае под денежным

потоком может пониматься экономия затрат, предотвращение убытков, а также дополнительный доход предприятия.

В качестве основного показателя, отражающего это соотношение, в экономической практике принято использовать функцию отдачи от инвестиций – Return on Investment, ROI .

$$ROI = NPV(R, d) + NPV(C, d)$$

где:

R – дополнительный денежный поток, создаваемый в результате реализации проекта;

C – затраты, связанные с реализацией проекта (расход ресурсов, отрицательная величина);

d – ставка дисконтирования;

NPV – функция дисконтирования.

Функция дисконтирования используется при анализе инвестиционных вложений для учета влияния фактора времени и приведения разновременных затрат к одному моменту (обычно моменту начала реализации проекта). Ставка дисконтирования в этом случае позволяет учесть изменение стоимости денег с течением времени.

Модель отдачи от инвестиций наглядно демонстрирует, какие две основные задачи необходимо решить при анализе любого инвестиционного проекта и, в частности, проекта по реализации мероприятий в сфере информационной безопасности: расчет затрат, связанных с проектом, и расчет дополнительного денежного потока. Если методология расчета совокупных затрат (C) за последние 10-15 лет в целом достаточно полно сформировалась (в виде концепции «Total Cost of Ownership», TCO – Совокупная стоимость владения, ССВ) и активно используется на практике применительно к различным видам информационных систем и элементам информационной инфраструктуры, то расчет дополнительного денежного потока (R), получаемого в результате инвестиций в средства защиты информации, как

правило, вызывает серьезные затруднения. Одним из наиболее перспективных подходов к расчету этого показателя является методика, которая опирается на количественную (денежную) оценку рисков ущерба для информационных ресурсов и оценку уменьшения этих рисков, связанного с реализацией дополнительных мероприятий по защите информации.

Таким образом, в целом состав методологии анализа целесообразности вложений средств в проекты, направленные на обеспечение информационной безопасности, схематично представлен на Рисунке 1.



Рисунок 1 – Структура методологии анализа эффективности вложений в проекты по УИБ

Анализ затрат, связанных с реализацией проекта, хотя и является относительно более простой задачей, все же может вызвать определенные затруднения. Так же как и для многих других проектов в сфере информационных технологий, анализ затрат на реализацию проектов в сфере информационной безопасности целесообразно осуществлять, опираясь на известную базовую методологию «Total Cost of Ownership» – ТСО (Совокупная стоимость владения – ССВ), введенную консалтинговой компанией «Gartner Group» в 1987 году применительно к персональным компьютерам. В целом, эта методика ориентирована на обеспечение полноты анализа издержек (как прямых, так и косвенных), связанных с информационными технологиями и информационными системами, в ситуациях, когда необходимо оценить экономические последствия внедрения и использования таких систем: при оценке эффективности инвестиций, сравнении альтернативных технологий, составлении капитальных и текущих бюджетов и пр.

В общем случае суммарная величина ССВ включает в себя:

- затраты на проектирование информационной системы;
- затраты на приобретение аппаратных и программных средств: вычислительная техника, сетевое оборудование, программное обеспечение (с учетом используемых способов лицензирования), а также лизинговые платежи;
- затраты на разработку программного обеспечения и его документирование, а также на исправление ошибок в нем и доработку в течение периода эксплуатации;
- затраты на текущее администрирование информационных систем (включая оплату услуг сторонних организаций, которым эти функции переданы на аутсорсинг);
- затраты на техническую поддержку и сервисное обслуживание;
- затраты на расходные материалы;
- затраты на телекоммуникационные услуги (доступ в Интернет, выделенные и коммутируемые каналы связи и пр.);

- затраты на обучение пользователей, а также сотрудников ИТ-подразделений и департамента информационной безопасности;

- косвенные затраты – издержки предприятия, связанные с потерей времени пользователями в случае сбоев в работе информационных систем.

Также в расчет затрат на повышение уровня информационной безопасности необходимо включить расходы на реорганизацию бизнес-процессов и информационную работу с персоналом: оплата услуг бизнес-консультантов и консультантов по вопросам информационной безопасности, расходы на разработку организационной документации, расходы на проведение аудитов состояния информационной безопасности и пр. Кроме того, при анализе расходов необходимо также учесть то обстоятельство, что в большинстве случаев внедрение средств защиты информации предполагает появление дополнительных обязанностей у персонала предприятия и необходимость осуществления дополнительных операций при работе с информационными системами. Это обуславливает некоторое снижение производительности труда сотрудников предприятия и, соответственно, может вызвать дополнительные расходы.

Значение ССВ в каждом конкретном случае необходимо определять индивидуально с учетом особенностей проекта, который предстоит реализовать: основной востребованной функциональности, существующей инфраструктуры, количества пользователей и других факторов. В общем виде ССВ для анализа эффективности и целесообразности вложений в реализацию проектов по повышению уровня защищенности информации определяется как сумма всех элементов затрат, скорректированная с учетом фактора времени:

$$NPV(C, d) = \sum_{t=0}^T \frac{\sum_{n=1}^N C_{tn}}{(1+d)^t}$$

где:

T – предполагаемый жизненный цикл проекта (информационной и/или организационной системы), лет;

N – количество видов затрат, принимаемых в расчет;

C_{nt} – затраты n -ого вида, понесенные в t -ом периоде, руб.

Таким образом, в целом могут быть определены затраты, связанные с реализацией мероприятий по обеспечению информационной безопасности. Однако наибольшую сложность представляет определение положительного эффекта от внедрения средств защиты информации. Как правило, эффект от внедрения информационных систем (ERP-систем, систем автоматизации бухгалтерского и управленческого учета, CAD/CAM-систем и пр.) определяется тем, что они обеспечивают автоматизацию и ускорение различных бизнес-операций, а это, в свою очередь, позволяет сократить затраты ручного труда, приобрести конкурентные преимущества и, таким образом, повысить общую эффективность хозяйственной деятельности. Однако внедрение средств защиты информации само по себе, как правило, не обеспечивает сокращения затрат (хотя в отдельных случаях может и обеспечить) – достижение положительного эффекта от их использования зависит от множества трудно контролируемых факторов как внутри предприятия, так и вне его. Более того, как уже было отмечено, реализация мероприятий, связанных с обеспечением информационной безопасности, может привести к дополнительным нагрузкам на персонал предприятия и, соответственно, к снижению производительности труда.

В связи с этим одним из немногих способов, которые могли бы помочь предприятию определить эффект от осуществления мероприятий в сфере защиты информации, является денежная оценка (хотя бы приблизительная) того ущерба, который может быть нанесен информационным ресурсам предприятия и который может быть предотвращен в результате реализации предлагаемых мероприятий. Таким образом, предполагаемый

предотвращенный ущерб (разница между предполагаемым ущербом в случае отказа от реализации мероприятий и ущербом в случае их реализации) будет составлять полученный экономический эффект – дополнительный денежный поток.

Очевидно, что при таком подходе большинство расчетов могут быть только оценочными и носить приблизительный характер. Это связано с тем, что активность злоумышленников, являющихся источниками угроз для информационной безопасности, практически непредсказуема: невозможно достоверно предсказать стратегии нападения, квалификацию нападающих, их конкретные намерения и ресурсы (финансовые, технические, организационные), которые будут задействованы для совершения тех или иных действий, а также намерения в отношении украденной информации (если целью атаки будет похищение конфиденциальных сведений). Соответственно, для осуществления всех необходимых расчетов необходимо сделать множество допущений и экспертных оценок в контексте деятельности данного конкретного предприятия, а также по возможности изучить статистическую информацию, касающуюся атак на информационные ресурсы, аналогичные защищаемым.

Таким образом, экономическая оценка эффективности мер по защите информации предполагает:

- оценку существующих угроз для информационных активов, которых коснется реализация защитных мер;
- оценку вероятности реализации каждой из выявленных угроз;
- экономическую оценку последствий реализации угроз.

Для осуществления такого анализа, как правило, используются следующие базовые понятия.

1) Оценочная величина единовременных потерь (Single Loss Expectancy, SLE_i) – предполагаемая средняя оценочная сумма ущерба в результате одного нарушения информационной безопасности i -го типа. Она может быть

определена как произведение общей стоимости защищаемых информационного активов (AV) на коэффициент их разрушения вследствие нарушения информационной безопасности (подверженности нападению), который обозначается EF_i (Exposure Factor).

2) Количество нарушений информационной безопасности за год (Annualized Rate of Occurrence, ARO_i) – оценочная частота, с которой в течение года происходят нарушения информационной безопасности (реализуются угрозы) i -го типа.

3) Оценочная величина среднегодовых потерь (Annualized Loss Expectancy, ALE_i) – суммарный размер потерь от нарушений информационной безопасности (реализации рисков) i -го типа в течение года.

$$ALE_i = SLE_i \times ARO_i = (AV \times EF_i) \times ARO_i$$

Непосредственный эффект от реализации мероприятий по повышению уровня информационной безопасности будет проявляться в том, что:

– негативные последствия каждого нарушения (каждой реализованной угрозы) после реализации мероприятий (EF'_i) будут меньше, чем были до их реализации: $EF_i > EF'_i$;

– частота нарушений информационной безопасности уменьшится после реализации мероприятий $ARO_i > ARO'_i$.

В результате уменьшенная величина ALE'_i будет составлять:

$$ALE'_i = SLE_i \times ARO'_i = (AV_i EF'_i) \times ARO'_i$$

Таким образом, суммарный годовой эффект от реализации мероприятия будет определяться как:

$$R = \Delta ALE_i = ALE_i - ALE'_i$$

Исходя из этого, общий денежный поток от реализации мероприятия определяется по следующей формуле:

$$NPV(R, d) = \sum_{t=0}^T \frac{\sum_{i=1}^I (ALE_{it} - ALE'_{it})}{(1 + d)^t}$$

На основе всех этих данных в соответствии с формулой может быть определен суммарный эффект от реализации мероприятий в сфере информационной безопасности и продемонстрировано, насколько оправданными и целесообразными являются вложения в те или иные средства защиты информации в условиях конкретного предприятия с учетом всех особенностей его функционирования (а также с учетом принятых допущений и сделанных предположений).

И хотя с математической точки зрения все расчеты в описанной рамочной модели оценки ROI являются предельно простыми, определение отдельных параметров (прогнозных частот нарушений и размеров потерь, а также предполагаемого срока использования программных и аппаратных средств и организационных моделей) может вызвать значительные затруднения на практике. Проведение таких расчетов, так же как и проведение аудитов информационной безопасности, может потребовать привлечения сторонних консультантов, однако квалификация и профессиональная специализация таких консультантов может существенно отличаться от квалификации консультантов, специализирующихся, например, на проведении аудитов и внедрении технических средств защиты информации. Причем если оценку вероятностей атак, а также оценку того, насколько эти атаки могут быть успешными, предпочтительно доверить внешним консультантам по информационной безопасности, то оценку стоимости информации и экономических последствий утраты контроля над информационными активами, скорее всего, целесообразно осуществлять самим специалистам, работающим на предприятии (экономистам, маркетологам и пр.), а также привлекать для этого сторонних специалистов из соответствующих сфер деятельности (маркетинга, финансов, торговли и пр.).

Несмотря на все трудности процесса оценки целесообразности внедрения средств защиты, описанная методология позволяет менеджерам и специалистам

по защите информации получать обоснованные оценки и делать формализованные выводы относительно того, насколько оправданными являются вложения в определенные средства защиты информации, а также определить основные приоритеты расходования средств, предусмотренных в бюджете на обеспечение информационной безопасности (если предприятие практикует выделение фиксированных сумм на эти цели). При этом достаточно высокий уровень достоверности таких оценок достигается за счет того, что вся работа по проведению оценки и подготовке инвестиционных решений раскладывается на несколько относительно более простых и «прозрачных» задач, решение каждой из которых может быть закреплено за специалистами в определенной сфере. В результате общая оценка складывается на основе полученных решений нескольких отдельных задач, каждое из которых может быть проконтролировано и при необходимости дополнительно уточнено. В этих условиях общее качество получаемой аналитической оценки и, соответственно, формулируемого решения зависит от квалификации всех экспертов, аналитиков и специалистов, участвующих в работе. А значит, одной из основных задач руководителей предприятия и менеджеров, отвечающих за обеспечение информационной безопасности и принятие решений в этой сфере, является подбор наиболее квалифицированных и опытных специалистов, ибо от качества их работы будет зависеть не просто безопасность отдельных элементов информационных активов в определенные моменты времени, а эффективность всей системы защиты информации в среднесрочной, а иногда и в долгосрочной перспективе.