

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.