В настоящее время во Франции существует специальное Министерство государственной службы, государственной реформы и децентрализации, в ее состав входит Генеральная дирекция администрации и государственной службы. Ее задачи контролировать соблюдение Общего устава (статута) государственной службы, собирать статистические данные, управлять соответствующим имуществом, руководить работой по реорганизации административных учреждений. Полномочия Генеральной дирекции распространяются на всех государственных служащих. Она участвует и в руководстве учебными заведениями по подготовке и переподготовке кадров для государственной службы.

В системе центральной государственной службы существует также ряд консультативных органов: Паритетные административные комиссии для каждого корпуса (штата) служащих, они занимаются вопросами продвижения по службе и следят за соблюдением дисциплины; Паритетные технические комитеты, занимающиеся организационными и уставными вопросами государственной службы; Комитеты гигиены и безопасности, создаваемые в каждом учреждении[1].

Н. А. Давлетханова
Уральский федеральный университет

РОЛЬ ОРГАНИЗАЦИОННЫХ МЕТОДОВ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

Проблема информационной безопасности остается актуальной в настоящее время, прежде всего из-за возрастающей роли информации в жизни современного общества. В связи с этим система ее защиты нуждается в постоянном развитии. Кроме того, развитие технических возможностей для несанкционированного доступа требует разрабатывать новые методы и способы его предотвращения.

Структуру защиты информации можно разделить на организационные методы и технические. И если технические зависят от разработки программного обеспечения компьютеров, их мощности и вида, то организационные составляют утвержденный алгоритм работы персонала, осуществляющего операции с защищенной информацией.

Информационная безопасность подразумевает решение ряда задач, таких как:

– формирование и совершенствование организационной структуры защиты информации, развитие научно-технических и кадровых возможностей;

– создание правовых, организационных и научно-технических условий для обеспечения защиты информации;

– обеспечение достаточно эффективной защиты информации;

[1] Зенков М. Ю. Зарубежный опыт управления: Государственная служба: Учебное пособие. Новосибирск, 2004. С. 55.

– создание эффективной и гибкой системы управления деятельностью системы защиты информации, приспособленной к постоянно изменяющимся условиям обстановки.

Для выполнения поставленных задач руководство разрабатывает стратегический план работы как для единичного достижения целей, так и для постоянного осуществления деятельности с защищаемой информацией.

Стратегия – комбинация из запланированных действий и быстрых решений по адаптации предприятия к новым возможностям получения конкурентных преимуществ и новым угрозам ослабления ее конкурентных позиций.

Основными целями при построении стратегии защиты информации стоит выделить конфиденциальность и целостность этой информации.

Конфиденциальность предполагает осуществление комплекса мер, обеспечивающих сохранность информации от лиц, не располагающих правом доступа к ней, либо определяющих частичный доступ в рамках их должностных полномочий и статуса.

Вторая цель – целостность – заключается в сохранности информации от различных искажений, порчи, изменений.

Основную роль в осуществлении организационных мер защиты информации играет руководство. В его задачи входит планирование мероприятий по созданию системы безопасности информации на предприятии, персональный контроль за исполнением утвержденных правил, утверждение списка сотрудников, имеющих доступ в той или иной скрываемой информации в соответствии с их должностными полномочиями, определение информации, подлежащей стать конфиденциальной.

Комплекс организационных мер защиты информации делится на несколько видов:

– организация работы с персоналом;

– организация пропускного режима внутри предприятия;

– планирование мероприятий по защите информации;

– осуществление аналитической работы и контроля[1].

Основные принципы организационной защиты информации:

– принцип комплексного подхода – эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

– принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);

– принцип персональной ответственности – наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения[2].

---

[1] Гришина Н. В. Организация комплексной защиты информации. М., 2007. С. 27.

[2] Жигулин Г. П. Организационное и правовое обеспечение информационной безопасности. СПб., 2014. С. 45.

При создании системы безопасности информации руководство использует несколько подходов. Один из них – изучение общей защищенности информации на данном этапе деятельности. Такой анализ направлен, прежде всего, на выявление отдельных документов либо групп документов, подлежащих конфиденциальности и особой сохранности от искажения и утраты.

Кроме того, руководство должно учитывать средства и возможности своего предприятия, а также значимость конфиденциальных документов и степень их использования в деятельности. Так, если компания повседневно связывает свою работу с защищаемой информацией, то средства и уровень контроля должны соответствовать. При этом стоит выделить отдельное подразделение, отвечающее за контроль над соблюдением всех норм и положений, установленных системой безопасности информации. И напротив, если конфиденциальная информация используется крайне редко и только в определенных случаях, то руководителю достаточно возложить обязанности контроля на какого-либо сотрудника.

Руководитель несет персональную ответственность за организацию и соблюдение установленных мероприятий, направленных на предотвращение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации. Он должен:

– знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки ценной информации;

– утверждать обязанности и задачи должностным лицам и структурным подразделениям в этой области;

– проявлять высокую требовательность к персоналу предприятия в вопросах сохранности конфиденциальной информации;

– оценивать деятельность должностных лиц и эффективность мероприятий по защите информации[1].

Организационные методы являются основополагающими при создании системы информационной безопасности. При их применении реализуются такие задачи как:

– создание эффективного механизма управления в учреждении;

– осуществление персональной ответственности, как первого руководителя компании, так и тех сотрудников, в чьи должностные обязанности входит работа с конфиденциальными сведениями;

– определение и утверждение перечня сведений, составляющих конфиденциальную информацию;

– ограничение лиц, имеющих доступ и допуск к секретной информации, и отражение этого решения в нормативно-правовых документах учреждения, предприятия;

[1] Громов Ю. Ю., Иванова О. Г., Мартемьянов Ю. Ф. Методы организации защиты информации. Тамбов, 2013. С. 28.

– подбор персонала, допускающегося к конфиденциальным сведениям, постоянное обучение сотрудников, поддержание благоприятных условий для работы, предоставление всех необходимых технических оснащений для осуществления деятельности с секретной информацией;

– осуществление систематического и строго контроля над соблюдением всех установленных норм и правил при работе с конфиденциальными сведениями.

Таким образом, можно заметить, что направленность и структуру системы защиты информации на предприятии определяют организационные методы. Они определяют круг лиц, осуществляющих деятельность в сфере безопасности информации, задачи, цели и тип системы, а также дает возможность подобрать необходимые технические средства с учетом требований и условий компании. Организационный подход устанавливает контроль и ответственность сотрудников при осуществлении свой работы.

О. И. Данченко
Пермский институт ФСИН России

РАЗВИТИЕ ГРАЖДАНСКОГО ОБЩЕСТВА И ГОСУДАРСТВА В НАЧАЛЕ XXI В.

Государство, бесспорно, является самым обширным и важным институтом, который имеет определенный механизм управления обществом для его нормального функционирования. Общество является неотъемлемой частью государства[1]. Что, прежде всего, понимается под обществом? Это определенный круг людей, связанный между собой общими интересами, желаниями, целями и т. д. Некоторые ученые не только современности, но и древних времен, считают, что общество есть «мать» государства. Мы полностью согласны с данной точкой зрения. Прежде всего, стоит вспомнить о том, что в начале образовывались семьи, которые разрастались. Через некоторый период времени образовался первобытнообщинный строй, в котором соответственно существовало общество, состоящее из первобытных людей. Затем образовалось общество охотников и собирателей. Государство было образовано лишь на определенном этапе развития общества. Соответственно, именно общество породило государство, для облегчения своей жизни. Рассматривая весь процесс развития государства, мы можем наблюдать, что на начальных стадиях государство полностью подавляло и подчиняло себе общество. На протяжении тысячелетий общество развивалось, обретало независимость и самосознание. Как же именно общество пришло к такому решению: просто сложившиеся обстоятельства или осознанное желание общества влиять на деятельность государства?

[1] Маргулян Я. А. Социальная политика: учебник. СПб., 2011.