ПРОБЛЕМА ПЕРСОНАЛА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

© О.П. Родин

Rodin O.P. The problem of staff in the sphere of information safety.

Информация, являясь продуктом деятельности, выступает как собственность государства, предприятий, учреждений, организаций, граждан и как объект собственности требует защищенности.

В основе системы информационной безопасности лежит человеческий фактор, предполагающий преданность персонала интересам фирмы и осознанное соблюдение им установленных правил защиты информации. Персонал фирмы, владеющий ценной и конфиденциальной информацией, работающий с конфиденциальными документами и базами данных, является наиболее осведомленным, трудно контролируемым и часто достаточно доступным источником для злоумышленника, желающего получить необходимые ему сведения [1–3].

По статистике 80 % случаев злоумышленных воздействий на информационные ресурсы совершаются людьми, имеющими непосредственное отношение к их эксплуатации. Такие действия совершаются либо под воздействием преступных групп (разведывательных служб), либо побуждаются внутренними причинами (зависть, месть, корысть и т. п.). Для блокирования угроз такого типа руководство организации с помощью службы безопасности должно осуществлять политику эффективного менеджмента, а именно, производить следующие организационные мероприятия:

– добывать всеми доступными законными путями информацию о своих сотрудниках, о людях или организациях, представляющих потенциальную угрозу информационным ресурсам;

– обеспечивать охрану сотрудников;

– устанавливать разграничение доступа к защищаемым ресурсам;

– контролировать выполнение установленных мер безопасности;

– создавать и поддерживать в коллективе здоровый нравственный климат.

Персонал является первостепенным и наиболее сложным элементом управления государственными и негосударственными структурами. В концепции экономической безопасности кадровая политика играет профилактическую роль по отношению к множеству видов угроз, исходящих от персонала, в том числе такой угрозы, как неблагонадежность отдельных сотрудников. В случае, если даже один сотрудник обманет доверие руководства, то никакие современные автоматизированные системы защиты не смогут гарантировать безопасность информации и предотвратить ее разглашение.

Следует отметить, что в современных предпринимательских структурах практически каждый основной сотрудник становится носителем ценных и конфиденциальных сведений, которые представляют интерес для конкурентов и криминальных сообществ. В связи с этим, помимо профессиональных способностей, сотрудники фирмы должны обладать высокими личными и моральными качествами. Они добровольно соглашаются на определенные ограничения в использовании информационных ресурсов и вырабатывают в себе самодисциплину, самоконтроль действий, поступков и высказываний.

Процессу приема сотрудника на работу, связанную с конфиденциальной информацией, предшествует ряд подготовительных аналитических этапов, которые позволяют составить точное представление о том, какой специалист и какой квалификации действительно нужен для данной должности, какими деловыми, личными и моральными качествами он должен обладать. Особенно это касается вновь вводимых должностей и новых направлений работы. На выходе процесса выполнения указанных подготовительных мероприятий составляется описание должности – вспомогательный документ, близкий по структуре должностной инструкции, который определяет всесторонние требования к кандидату на должность.

Поиск кандидата на вновь создаваемую или вакантную должность в фирме не должен носить бессистемный характер. Случайный, неизвестный фирме человек в определенной степени таит опасность как с точки зрения его профессиональной пригодности, так и личных качеств. Особенно большие сомнения вызывает подобный метод при подборе кандидатов на должности, связанные с владением конфиденциальной информацией. Тем не менее не следует отказываться от подобного метода, потому что случайный человек может оказаться идеальной кандидатурой по всем критериям. Но дело в том, что этот метод не должен быть единственным. К числу других методов можно отнести следующие:

1. Поиск кандидата внутри фирмы, особенно если речь идет о руководителе, специалисте высокого уровня или сотруднике, работа которого будет связана с владением тайной фирмы. Этот метод дает возможность продвигать способных сотрудников по служебной лестнице и заинтересовывать подобной перспективой всех сотрудников фирмы. Перераспределение персонала в соответствии с его склонностями, профессиональной грамотностью и преданностью делам фирмы всегда дает большой положительный рост эффективности работы фирмы и с достаточной степенью гарантии обеспечивает ее информационную безопасность.

Большим преимуществом этого метода является то, что о кандидате достаточно много известно всему кол-

лективу фирмы и судить о его профессиональных и личных качествах, соответствии предлагаемой должности можно на основании достаточного широкого круга мнений.

С другой стороны, использование данного метода может существенно подорвать дисциплину внутри подразделения в силу все той же известности соискателя. Персоналу подразделения очень трудно воспринять человека, проработавшего с ними определенное количество времени на равном положении как непосредственного руководителя.

2. Поиск кандидатов среди студентов и выпускников учебных заведений, установление связей с подразделениями вузов, занятыми трудоустройством выпускников. Можно иметь достаточно полную информацию о профессиональных, личных и моральных качествах студентов. Очень эффективно вести поиск (даже на средних курсах) наиболее способных студентов, привлекать их в процессе учебы к работе в фирме.

3. Обращение в государственные и частные бюро, агентства по найму рабочей силы, биржи труда, службы занятости, организации по трудоустройству лиц, уволенных по сокращению штатов, трудоустройству молодежи, бывших военнослужащих и т. п. Подобные агентства, помимо целенаправленного поиска необходимых специалистов высокой квалификации, организуют переподготовку специалистов по заказу фирмы, в том числе одновременно в области обеспечения информационной безопасности фирмы.

4. Рекомендации работающих в фирме сотрудников. Обычно такие рекомендации отличаются ответственным и взвешенным характером, т.к. с рекомендуемыми людьми сотрудникам придется работать вместе.

При подборе сотрудников для работы с конфиденциальной информацией важно не только определить пути поиска кандидатов, но и установить правовое обоснование тех ограничений во владении и использовании информации, которые неминуемо касаются данных сотрудников.

В организации, работающей с конфиденциальной информацией, обязательно разграничение доступа к информационным ресурсам. В случае предательства или других злоумышленных действий сотрудника ущерб должен быть ограничен рамками его компетенции. Сотрудники учреждения должны знать, что выполнение установленных правил контролируется руководством и службой безопасности.

ЛИТЕРАТУРА

1. *Лукацкий А.В.* Подготовка кадров в области защиты информации // Системы безопасности, связи и телекоммуникаций. 1997. № 5.
2. *Лукацкий А.В.* Кадры решают все // Системы безопасности, связи и телекоммуникаций. 1997. № 6.
3. *Степанов Е.А.* Персонал в системе защиты информации. М., 2002.

Поступила в редакцию 16 октября 2006 г.

ЗАЩИТА ПЕРЕДАЧИ ДАННЫХ ОТ СЛУЧАЙНЫХ И ПРЕДНАМЕРЕННЫХ ПОМЕХ

© Н.В. Седова

Sedova N.V. Protection of the data transmission from accidental and deliberate interference.

Современное развитие экономики и политики характеризуется все большей зависимостью от информационных потоков. Идет постоянная борьба между конкурирующими группами во всех сферах человеческой деятельности, и все большее применение в этой борьбе находят новые средства и методы информационного противостояния. Несмотря на создание сложнейших систем и средств защиты информации (в том числе и систем защиты передачи данных), их уязвимость не уменьшается, а наоборот, все более возрастает. Это приводит к возникновению эффекта «снежного кома», когда один маленький комок снега приводит к сходу лавины. Чем оригинальнее идея и техническое воплощение средств защиты, тем изощреннее способы ее взлома.

Различают две основные группы методов решения задач защиты передачи данных: канально-ориентированные и межконцевые методы защиты. Канально-ориентированные методы защиты передачи данных основываются на предположении, что узлы системы передачи данных (СПД) не подвергаются несанкционированному доступу, что гораздо проще и «выгоднее» получить необходимую информацию, передаваемую по отдельному каналу связи. Межконцевые методы защиты СПД, напротив, защищают сообщения в процессе передачи данных между узлами источника и приемника таким образом, что при раскрытии одного из каналов между источником и адресатом не происходит раскрытия всего потока сообщений.

Анализ потока сообщений проводится, как правило, по значениям длин частот сообщений разных классов, адресов источника и адреса потока сообщений. Следовательно, защита строится на возможности их сокрытия.

При применении канального шифрования обеспечивается передача непрерывного потока данных по каналу от одного узла к другому. Это обеспечивает сокрытие значений частоты и длительности соединения, но при этом при вскрытии узла весь поток сообщений может быть подвергнут анализу.

Наиболее глубокий анализ данных, передаваемых через узлы СПД, обеспечивает контекстный анализ. Он позволяет, с одной стороны, предотвратить утечку конфиденциальной информации с доступных ресурсов, а с другой – исключить поступление потенциально опасных сообщений и перегрузку систем передачи данных. Из имеющихся средств контекстного анализа в качестве примера можно указать антивирусные реше-