УДК 331.5; 658.3

РАБОТА С ПЕРСОНАЛОМ В РАМКАХ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Н.П. Лонцих[1], Е.П. Кунаков[2]
Иркутский национальный исследовательский технический университет,
664074, Россия, г. Иркутск, ул. Лермонтова, 83.
Статья посвящена актуальной на сегодняшний день проблеме защиты информации, организации системы защиты информации и работе с персоналом в рамках системы защиты информации. В статье рассматриваются ключевые этапы работы с персоналом. Обоснована необходимость постоянной, планомерной работы с персоналом организации в рамках системы защиты информации.
Ключевые слова: защита информации; система защиты информации; управление персоналом; методы управления персоналом; персонал.

PERSONNEL POLICY WITHIN INFORMATION SECURITY SYSTEM IN THE ORGANIZATION
N. Lontsikh, E. Kunakov
Irkutsk National Research Technical University,
83 Lermontov Str., Irkutsk, Russia, 664074.
The article is devoted to a challenging issue of the information protection, organization of in-formation security systems and personnel policy within the information security system. The article discusses the key stages of work with personnel having access to the information. The authors reason the necessity of constant, systematic operation of personnel policy within the information security system.
Keywords: information security; information protection system; personnel management; per-sonnel management methods; staff.

Информация является одним из наиболее ценных ресурсов компании, поэтому обеспечение защиты информации является одной из важнейших и приоритетных проблем. Традиционно система защиты информации рассматривается как совокупность программных, программно-аппаратных и технических средств защиты информации (антивирусов, межсетевых экранов, систем обнаружения вторжений, систем контроля доступа и т. п.) При построении такой системы защиты информации в большинстве случаев учитываются лишь технологические угрозы информационной безопасности. Однако в данных системах остается одно уязвимое место – собственный персонал компании, обладающий доступом к различным конфиденциальным сведениям организации. Очевидно, что надежность защиты информации напрямую зависит от системы защиты данной информации. В теории под системой защиты информации понимают рациональную совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению. На сегодняшний день на основе накопившегося опыта разработан ряд методологий построения системы информационной безопасности:

- *Стандарты ISO 27001 (ISO 17799);* [1]

Стандарт ISO/IEC 27001:2005 представляет собой перечень требований к системе менеджмента информационной безопасности, обязательных для сертификации, а стандарт ISO/IEC 17799:2005 выступает в качестве руководства по внедрению, которое может использоваться при проектировании механизмов контроля, выбираемых организацией для уменьшения рисков информационной безопасности.

Стандарт ISO 27001 определяет информационную безопасность как: «сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность».

Стандарт ISO 27001 определяет процессы, представляющие возможность бизнесу устанавливать, применять, пересматривать, контролировать и поддерживать эффективную систему менеджмента информационной безопасности; устанавливает требования к разработке, внедрению, функционированию, мониторингу, анализу, поддержке и совершенствованию документированной системы менеджмента информационной безопасности в контексте существующих бизнес рисков организации.

Наряду с элементами управления для компьютеров и компьютерных сетей, стандарт уделяет большое внимание вопросам разработки политики безопасности, работе с персоналом (прием на ра-

[1] Лонцих Наталья Павловна, кандидат педагогических наук, доцент, e-mail: palon@list.ru
Lontsikh Natalia, Candidate of Pedagogy, Associate Professor, e-mail: palon@list.ru
[2] Кунаков Егор Петрович, аспирант, e-mail: egor-kunakov@mail.ru
Kunakov Yegor, a postgraduate student, e-mail: egor-kunakov@mail.ru

боту, обучение, увольнение с работы), обеспечению непрерывности производственного процесса, юридическим требованиям.

• *Требования акта Сарбанеса-Оксли (США) SOX;* [2]

Акт Сарбейнса – Оксли (SOX), принятый в 2002 году, выдвигает требования для фирм, представленных на американских фондовых биржах. Взаимосвязь между актом SOX и информационной безопасностью неочевидна - основная задача акта — обеспечить точность и целостность информации о финансовой отчетности публичных компаний. Поскольку в абсолютном большинстве случаев эта информация собирается с помощью автоматизированных систем, SOX автоматически выдвигает требования к их защищенности. В противном случае говорить о целостности и тем более точности каких-либо данных абсолютно невозможно. Самая «страшная» секция закона SOX получила культовый номер 404, который до выхода акта ассоциировался исключительно с интернет-страницами. В этой секции описывается ответственность руководства компании за установление «внутреннего контроля над ведением финансовой отчетности».

В рамках этой ответственности руководство компании обязано «обеспечить разумные гарантии предотвращения или своевременного обнаружения случаев несанкционированного приобретения, использования или перемещения активов зарегистрированного лица, которые могут существенно повлиять на финансовую отчетность». А поскольку в категорию «активы» входит вся конфиденциальная информация компании, руководство обязано обеспечить ее сохранность.

• *Стандарт Банка России СТО БР ИББС-1.0-2014;* [3]

Стандарт Банка России является рекомендательным документом, который в некоторых случаях становится обязательным. В данном стандарте указывается, что «наибольшими возможностями для нанесения ущерба [организации]… обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является нецелевое использование предоставленного контроля над информационными активами, а также сокрытие следов своей деятельности. Внешний злоумышленник скорее да, чем нет, может иметь сообщника(ов) внутри организации».

Для защиты банка от собственных сотрудников стандарт предлагает использовать эффективную политику ИТ-безопасности. В стандарте раскрываются основные черты этой политики, связанные с принципами антивирусной защиты, доступом в глобальную сеть, разделением ролей и т. д. Другими словами, в стандарте содержатся конкретные рекомендации для создания действительно защищенной ИТ-инфраструктуры.

• *Отраслевые стандарты предприятий.*

Основной идеей всех стандартов является положение о том, что большинство проблем информационной безопасности лежит внутри компании, а не за ее пределами. Некоторые документы (например, стандарт ЦБ) указывают на это явно, другие говорят об этом косвенно.

Каждая методология включает рекомендации, как по организационным, так и по техническим мерам обеспечения безопасности. Помимо выполнения внутренних проверок (аудитов) своими силами, предприятия проводят комплексный аудит информационной безопасности с помощью третьих сторон, что повышает эффективность системы защиты информации. В основе процессного подхода западных стандартов лежит также непрерывный контроль и совершенствование уже существующих мер.

В любой системе защиты информации, будь она в крупной или небольшой организации, используются различные средства обеспечения безопасности, среди которых можно выделить следующие [4].

Технические средства. К ним относятся охранные системы, видео-радиоаппаратура, заграждения и т. д.

Организационные средства. Создание специализированных отделов, обеспечивающих безопасность предприятия.

Информационные средства. Наглядная информация по вопросам сохранения конфиденциальной информации. Кроме этого, важнейшая информация для принятия решений по вопросам безопасности сохраняется в компьютерах.

Финансовые средства. Без достаточных финансовых средств невозможно функционирование системы безопасности, вопрос лишь в том, чтобы использовать их целенаправленно и с высокой отдачей.

Правовые средства. Создание локальных правовых актов (стандартов предприятия) по вопросам обеспечения безопасности и использование изданных вышестоящими органами власти законов и подзаконных актов

Кадровые средства. Подбор компетентного персонал и повышения их профессионального мастерства в этой сфере информационной безопасности.

Интеллектуальные средства. Привлечение к работе высококлассных специалистов, научных работников (иногда целесообразно привлекать их со стороны) позволяет внедрять новые системы безопасности.

Применение каждого из указанных средств в отдельности не дает необходимого эффекта, он возможен только на комплексной основе.

Основные этапы по защите информации на предприятии

В современных компаниях практически любой сотрудник становится носителем ценных сведений, которые представляют интерес для конкурентов. Разглашение конфиденциальной информации может нанести существенный ущерб организации, и не только экономический.

Основные этапы защиты информации зависят от того, как организована система защиты информации. Для этого высшему руководству необходимо:

- разработать перечень информации, относящейся к защищенной;
- ограничить и регламентировать доступ к носителям информации;
- определить круг лиц, имеющих право доступа к информации;
- нанести на документы, составляющие коммерческую тайну, соответствующие надписи или пометки (при этом необходимо указывать обладателя информации, его местонахождение и наименование);
- ознакомить работников с локальными актами о коммерческой тайне;
- внести в трудовые договоры, особенно с вновь принимаемыми лицами, пункт об обязательстве работника не разглашать определенную информацию.

В деле защиты информации организации от различного вида угроз значительное место занимает персонал предприятия, который может стать как объектом, так и субъектом таких угроз. Необходимо внедрять такую систему управления персоналом, которая бы помогала в деле обеспечения информационной безопасности, играла профилактическую роль по отношению к угрозам. [5]

Формы реализации угроз информационной безопасности предприятия разнообразны по своему характеру и содержанию, что затрудняет процесс противодействия им. При этом мотивация сотрудников при разглашении конфиденциальной информации может быть различна. Реализация мер кадровой службы по защите информации организации предполагает планирование, организацию, мотивацию и контроль персонала в целях создания системы обеспечения информационной безопасности.

Одним из наиболее важных направлений в деятельности руководства является постоянная работа с персоналом предприятия, имеющим в силу своих должностных обязанностей доступ к конфиденциальной информации. Персонал, постоянно работающий со сведениями конфиденциального характера (их носителями), — основной субъект в сфере защиты информации. Одновременно он и единственный ее «нематериальный носитель». Работа с персоналом подразумевает целенаправленную деятельность высшего руководства и персонала организации по предотвращению ситуаций разглашения защищенной информации организации.

Высокий уровень подготовки сотрудников предприятия в вопросах защиты конфиденциальной информации позволит максимально снизить вероятность появления непреднамеренных ошибок в обращении с этой информацией. И наоборот, проявление сотрудниками предприятия низких профессиональных навыков значительно снизит эффективность системы защиты конфиденциальной информации на предприятии в целом, так как никакие меры организационного и технического характера не скомпенсируют возможную утечку информации со стороны сотрудников предприятия.

Причинами разглашения конфиденциальной информации персоналом предприятия чаще всего становятся следующее:

- недостаточный уровень знаний нормативных актов и внутренних документов предприятия, регламентирующих деятельность по защите информации;
- слабый контроль со стороны руководителей всех уровней за состоянием защиты информации и эффективностью принимаемых мер по недопущению разглашения этой информации;
- недостаточное внимание к вопросам организации работы с персоналом предприятия, изучению морально-деловых качеств сотрудников;
- несвоевременное принятие эффективных действий по предотвращению разглашения конфиденциальной информации, а также нарушений норм и правил защиты информации сотрудниками.

Наряду с перечисленным причинам к разглашению информации могут также привести различные экстремальные ситуации, чрезвычайные происшествия, локальные неисправности в системах коммуникации и жизнеобеспечения. В таких ситуациях охраняемая информация потенциально может использоваться лицами, не допущенных к ней. В связи с этим важно иметь необходимую информацию о лицах, не являющихся сотрудниками предприятия, которым предоставлено право его посеще-

ния (нахождения на его территории) для решения различных вопросов и задач. Заблаговременно определяется круг таких лиц, включающий прежде всего:

- сотрудников организаций-партнеров и других взаимодействующих с предприятием;
- работников органов государственной власти, местного самоуправления, территориальных и надзорных органов;
- представителей средств массовой информации (СМИ);
- работников коммунальных служб;
- работников обслуживающих инфраструктуру организации;
- инкассаторов, сотрудников банковских структур, подразделений федеральной почтовой связи. [5]

Работа с персоналом предприятия высшим руководством должна проводиться в плановом порядке, на постоянной основе. Неотъемлемой частью этой работы является распределение высшим руководством задач и функций между должностными лицами и структурными подразделениями, определение приоритетности и очередности выполнения этих функций и задач.

В зависимости от размера организации непосредственное участие в работе с персоналом предприятия, как правило, принимают служба кадров, служба безопасности, режимно-секретное подразделение, юридическая служба (юрисконсульт), служба охраны и служба собственной безопасности.

Высшее руководство и сотрудники, использующие в своей работе конфиденциальную информацию, могут в своей деятельности опираться на Федеральный закон "О коммерческой тайне" [6]. Данный закон составляет правовую основу организации и проведения работы с персоналом предприятия, допущенным к сведениям, в установленном порядке отнесенным к коммерческой тайне.

В нем закреплен принцип добровольности доступа к коммерческой тайне работника предприятия. Установлены обязанности работодателя по отношению к сотруднику предприятия в связи с охраной конфиденциальности информации, составляющей коммерческую тайну.

Согласно этому закону высшему руководству предприятия необходимо:

- ознакомить под расписку работника с перечнем информации, составляющей коммерческую тайну;
- ознакомить под расписку работника с установленным режимом коммерческой тайны в организации и с мерами ответственности за его нарушение;
- создать работнику необходимые условия для соблюдения установленного режима коммерческой тайны.

Этапы работы с персоналом в рамках системы защиты информации

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 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 средств защиты информации.

Поэтому работа с сотрудниками в системе защиты информации должна проводиться в несколько этапов:

- при приеме на работу или переводе на должность, связанную с доступом к конфиденциальной информации;
- в ходе выполнения должностных обязанностей;
- во время прекращения выполнения сотрудником его должностных обязанностей (увольнение или перевод на другую должность).

Усилия высшего руководства предприятия должны быть сосредоточены на следующих направлениях:

- изучение личностных качеств сотрудников;
- повышение ответственности сотрудников за сохранение защищаемой информации;
- проведение профилактической работы по предупреждению случаев раскрытия защищённой информации;
- повышение уровня теоретических знаний и практических навыков сотрудников в вопросах защиты информации;
- создание и поддержание устойчивого морально-психологического климата в коллективе;
- создание и применение системы стимулирования труда.

Один из наиболее важных этапов в работе с персоналом предприятия — процесс подбора сотрудников для назначения на должности, связанные с защищаемой информацией. При подборе руководством проводится оценка соответствия требованиям:

- по уровню подготовки и квалификации, наличию необходимого опыта работы;
- по морально-деловым и личностным качествам, степени ответственности за принимаемые управленческие и исполнительские решения (в зависимости от занимаемой должности).

В число основных методов оценки соответствия предъявляемым требованиям входят:

- изучение материалов личного дела, персональных данных, резюме и иных документов;
- проведение собеседования;
- проведение тестирования.

На основе изучения материалов личного дела и документов, а также результатов собеседования формируется вывод об оценке соответствия предъявляемым требованиям. Результаты тестирования позволяют определить уровень подготовленности к выполнению должностных обязанностей, в том числе знание положений нормативно-методических документов, и имеющиеся практические навыки работы по данной специальности.

При подборе кандидатов для назначения на должности, связанные с конфиденциальной информацией, в обязательном порядке учитывается уровень каждой конкретной должности с точки зрения реализации управленческих решений, выполнения функций и задач деятельности предприятия. Исходя из данных критериев, такие должности подразделяют на следующие группы:

- должности руководителей предприятия (высшее руководство предприятия);
- должности заместителей руководителя;
- должности руководителей структурных подразделений;
- должности руководителей служб безопасности и их заместителей;
- должности сотрудников служб безопасности предприятия;
- должности сотрудников предприятия, осуществляющих работу с конфиденциальной информацией. [4]

При отборе сотрудников для назначения на перечисленные должности дополнительно учитывается объем и важность доступных сведений конфиденциального характера.

Такого рода анализ необходим как в отношении специалистов и руководителей, которые работают с информацией, подлежащей защите, в связи с выполнением своих должностных обязанностей, так и специалистов и руководителей, чьей основной задачей является обеспечение информационной безопасности предприятия.

Особенности подбора, приема и оформления на работу кандидатов для назначения на должности, связанные с допуском к государственной тайне, определены в Постановлении правительства РФ «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» [6]. В данной инструкции конкретизированы функции, возлагаемые на службу кадров предприятия.

В ходе собеседования наряду с уточнением отдельных вопросов анкеты, заполняемой при оформлении материалов на допуск к государственной тайне, выясняют также следующие вопросы:

- имел ли гражданин за последний год отношение к секретным работам, документам и изделиям;
- давал ли он обязательство по неразглашению сведений, составляющих государственную тайну;
- работал ли (служил) на режимных объектах.

После принятия решения о назначении сотрудника, руководитель структурного подразделения и сотрудник службы защиты информации (службы безопасности) проводят вводный инструктаж. В ходе инструктажа обговариваются должностные обязанности, положения нормативно-методических и внутренних организационно-распорядительных документов, регламентирующих вопросы защиты конфиденциальной информации на предприятии.

Приведенный перечень этапов не является исчерпывающим и, в зависимости от специфики деятельности предприятия, степени защиты используемой информации, объема выполняемых работ, а также опыта работы в области защиты информации, может быть дополнен иными.

Защищаемая информация - это информация, доступ к которой имеет ограниченный круг лиц, не подлежащая как предоставлению - передаче определенному кругу лиц, так и распространению. Любая несанкционированная передача данной информации нарушает установленный режим защиты информации и снижает ценность такой информации.

Библиографический список

1. Стандарт ГОСТ Р ИСО 27001–2005. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М. : СТАНДАРТИНФОРМ, 2005. 31 с.

2. Основы аудита / под ред. д-ра экон. наук, проф. Р.П. Булыги. – Ростов н/Д: Феникс, 2010. – 317 с.

3. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения: стандарт Банка России (СТО БР ИББС-1.0-2014).

4. Аверчиков В.И., Рытов М.Ю. Служба защиты информации – организация и управление: учеб. пособие для вузов. – М.:ФЛИНТА, 2011. – 186 с.

5. Погодина И.В. Если работник не умеет хранить деловые секреты // Трудовое право. – 2009. –№ 10. – С. 23–42.

6. О коммерческой тайне: федер. закон от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014).