обеспечения информационной безопасности. Планирование персонала - это подбор персонала и оформление допуска для работы с конфиденциальной информацией. Организация - обучение сотрудников правилам и приемам работы с конфиденциальной информацией. Мотивация сотрудников в обеспечении информационной безопасности реализуется путем поощрения и с помощью применения специальных санкций за соответствующие нарушения. Контроль над сотрудниками предприятия должен носить комплексный и непрерывный характер [1].

В области подготовки кадров по вопросам защиты информации Соединенные Штаты являются одной из передовых стран. В нашей стране широко используется опыт США и других передовых стран для подготовки кадров широкого профиля по комплексной защите информации с узкой специализацией по одному из направлений защиты информации.

Мы должны научиться дорожить информацией. Каждый специалист в области защиты информации должен понимать важность решаемой им задачи, осознавать ответственность перед обществом и своей компанией.

В Соединенных Штатах при приеме сотрудника в службу безопасности досконально изучается его характер, окружение, прошлое, семья и др. Помимо простого анкетирования, проводится ряд тестов на профессиональную пригодность, определяются положительные и отрицательные черты характера. Таким образом, возможность попадания в службу безопасности случайных людей сводится до минимума. Большое воздействие на сотрудника имеет материальное обеспечение. При хорошей зарплате сотрудников вероятность хищения информации, представляющей ценность для конкурентов, минимальная. Опираясь на положительный опыт в защите информации в США, в нашей стране можно создать четкую и отлаженную систему организации работы с кадрами, способную защитить секреты предприятия [1].

1. Гимбицкая Л.А., Гимбицкий В.А., Демурчев Н.Г. Организационная защита информации. Учебное пособие. Ставрополь: СГУ, 2011. – 120 с.
2. Алавердов А.Р. Управление кадровой безопасностью организации. М.: Маркет ДС, 2008. – 213 с.

Гимбицкий В.А., Гимбицкая Л.А.
Опыт зарубежных стран в управлении персоналом

*Краснодарское высшее военное авиационное училище летчиков
(Россия, Краснодар)*

doi: 10.18411/lj-10-2020-03

idsp: ljjournal-10-2020-03

Аннотация

В данной статье рассмотрены проблемы управления персоналом, сохранения конфиденциальной информации предприятия в ведущих зарубежных странах. Выявлена и обоснована необходимость особого отношения к личности сотрудника. На основе проведенного исследования авторами предлагается взять за основу использование упреждающих и текущих мероприятий, направленных на работу с персоналом.

Ключевые слова: защита информации, информационная безопасность, информационные сети, хищение информации, утечка информации, доступ к конфиденциальной информации.

Abstract

This article discusses the problems of personnel management, maintaining confidential information of the enterprise in leading foreign countries. The need for a special attitude to

the employee's personality is identified and justified. Based on the research, the authors suggest using proactive and ongoing measures aimed at working with staff as a basis.

Keywords: information protection, information security, information networks, information theft, information leakage, access to confidential information.

Актуальность проблемы защиты информации в современном мире информационных технологий очень высока. Разветвлённые компьютерные сети и телекоммуникации обеспечивают хранение, обработку и предоставление информации потребителям, и высокая степень автоматизации жизни современного общества порождает риск снижения информационной безопасности как личной, так государственной и корпоративной. Доступное и широкое распространение современных информационных технологий и компьютеров делает их уязвимыми со стороны преступных структур. Субъекты информационных отношений потенциально подвержены нанесению им ущерба как морального, так и материального через воздействие на важную для них информацию и её носители, а также через неправомерное использование подобной информации. В Федеральном бюро расследований (США) проведены исследования, в ходе которых установлено, что каждые 20 секунд в США совершается преступление с использованием программных средств, 80% подобных преступлений происходит через сеть *Internet*. Потери от хищений или повреждений компьютерных сетей превышают 100 млн. долл. в год [2]. Обеспечить информационную безопасность - значит гарантировать удовлетворение законных прав и интересов субъектов информационных отношений. Все субъекты информационных отношений заинтересованы в обеспечении своей информационной безопасности. И в условиях высокоавтоматизированных технологий и связанной с ними проблемой защиты информации сейчас в современных зарубежных компаниях повышено внимание к кадрам и методам управления ими. На современных предприятиях создаются эффективные системы защиты конфиденциальной информации, а также системы отслеживания того, как персонал соблюдает соответствующие правила, системы санкций, применяемые к нарушителям при угрозе умышленной и неумышленной утечки информации. Главный субъект реализации угроз информационной безопасности на предприятии – его персонал. Персонал предприятия, являясь одним из основных носителей информации, становится и главным источником утечки сведений с использованием таких методов, как подкуп, переманивание сотрудников (около 43% вероятности утечки информации), выведывание информации (24%) [2]. По данным западных специалистов по обеспечению экономической безопасности, правильный подбор, расстановка и воспитание персонала на 80 % обеспечивает надёжную сохранность коммерческой тайны [3]. Защитить информацию, составляющую коммерческую тайну предприятия, возможно с использованием упреждающих и текущих мероприятий, направленных на работу с персоналом. При этом персонал может стать как объектом, так и субъектом угроз информационной безопасности [1]. Ключевые принципы и правила управления персоналом с учетом требований информационной безопасности определены в международном стандарте ISO/IEC 17 799:2000 и сводятся к необходимости выполнения определенных требований безопасности, повышения осведомленности сотрудников и применения мер пресечения к нарушителям [4]. Для создания эффективной системы защиты разработан ряд стандартов. Главная задача стандартов информационной безопасности — создать основу для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий. Наиболее значимыми стандартами информационной безопасности в мире являются: Критерии безопасности компьютерных систем Министерства обороны США («Оранжевая книга»), Руководящие документы Гостехкомиссии России, Европейские критерии безопасности информационных

технологий, Федеральные критерии безопасности информационных технологий США, Канадские критерии безопасности компьютерных систем и Единые критерии безопасности информационных технологий [1]. Мировыми стандартами определены основные формы реализации угроз информационной безопасности. В первую очередь, это перехват конфиденциальной информации при помощи различных методов – от простого подслушивания разговоров сотрудников фирмы до использования технических подслушивающих устройств, копирования документов и электронных баз данных. Далее следует хищение конфиденциальной информации, в результате чего предприятие навсегда лишается её. Ущерб предприятию наносит и преднамеренное повреждение и уничтожение информации работником, причиной которого может стать личная месть работодателю. Искажение нелояльным сотрудником конфиденциальной информации может стать причиной принятия неверного управленческого решения специалистами предприятия [2]. Специалисты по защите информации разных стран пристально изучили механизмы и факторы, обеспечивающие высокую эффективность развития экономики Японии на протяжении длительного периода. Анализ показал, что в центре японской концепции управления находится человек, который рассматривается как наивысшая ценность для фирмы. Исходя из этой теории, все системы управления нацелены на развитие разнообразных способностей работников для того, чтобы они были в максимальной степени использованы в процессе производства, а человек стремился к процветанию фирмы, в которой работает [3].

Стратегические концепции управления кадрами в промышленно развитых странах рассматривают работников как решающий фактор сохранения конкурентоспособности и нацелены на подготовку кадров в соответствии с изменяющимися требованиями рынка и с учетом введения новых технологий. В последнее время в США и европейских странах с учетом японского опыта разработаны различные модели управления, в центре которых – человек. Эти модели содержат следующие основные блоки: персонал организации; тщательный учет знаний и способностей работников при назначении их на ключевые должности в фирме; стиль и культура деловых взаимоотношений в данной организации; долгосрочные цели развития фирмы [1]. Набором и отбором кадров на зарубежных предприятиях занимаются отделы управления персоналом, а служба безопасности контролирует этот процесс. Анализ рабочего места будущего работника проводят в период предварительного отбора: составляется психологический портрет идеального сотрудника, подходящего для выполнения всех функциональных обязанностей на данной должности. Отбор будущих работников осуществляется после анализа рабочего места и набора определённого количества претендентов: из ряда заявителей компетентные органы предприятия выбирают одного претендента, который наиболее полно соответствует предъявленным требованиям на вакантное место. Раньше отбор претендентов на предприятиях США осуществлялся интуитивно, в соответствии с личными пристрастиями работодателя. Сегодня в США кандидату на вакантное рабочее место необходимо пройти несколько ступеней профессионального отбора, среди них: предварительная беседа по отбору, заполнение бланка заявления, беседа по найму, тесты по найму, проверка рекомендаций и обязательств перед другими фирмами, медицинский осмотр, принятие решения [3]. В США действуют специальные организации, которые получают рекомендации на претендентов на вакантные рабочие места с прежних мест работы и собирают обобщённый портрет претендента. Закон Соединённых Штатов строго следит, чтобы добываемая информация не нарушала права человека и предоставлялась только лицам, непосредственно принимающим участие в отборе кандидатов. Собирать информацию на потенциальных работников стало возможно в США ещё в 1977 году, когда департамент США разрешил 50 штатам предоставлять доступ к информации о кандидатах на работу из судов, фактах арестов и других эпизодах биографии [4]. При этом претендент на работу должен быть

оповещен заранее о проводимом исследовании. Также в обязательном порядке претенденту сообщают причину отказа в должности. За ним сохраняется право пересмотра информации, из-за которой ему отказали в назначении.

1. Гимбицкая Л.А., Гимбицкий В.А., Демурчев Н.Г. Организационная защита информации. Учебное пособие. Ставрополь: СГУ, 2011. – 120 с.
2. Алавердов А.Р. Управление кадровой безопасностью организации. М.: Маркет ДС, 2008. – 213 с.
3. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: Учеб. пособие. М.: ФОРУМ, 2009. – 435 с.
4. Столяров Н. В. Зарубежный опыт защиты информации в процессе организации работы с кадрами (на примере США) // Безопасность для всех, 2010. – 654 с.

Горбачев А.Ю., Гулякин Д.В.
Виртуальное строительство (цифровая модель здания)

*Кубанский государственный технологический университет
(Россия, Краснодар)*

doi: 10.18411/lj-10-2020-04

idsp: ljournal-10-2020-04

Аннотация

Грамотное использование BIM технологий позволяет рассчитать и определить практически все аспекты строительства еще до непосредственного начала строительных работ на объекте, создать 3D-модель здания, включая все сопутствующие конструкции и коммуникации для наглядного представления проекта заказчику и иным лицам. Все это в той или иной степени повышает производительность труда различных субъектов управления строительством.

Ключевые слова: технологии, строительство, BIM, моделирование, конструкции, модель, здание, эксплуатация.

Abstract

The competent use of BIM technologies allows you to calculate and determine almost all aspects of construction even before the direct start of construction work at the facility, create a 3D model of the building, including all related structures and communications for a visual presentation of the project to the customer and other persons. All this to one degree or another increases the labor productivity of various subjects of construction management.

Keywords: technology, construction, BIM, modeling, construction, model, building, operation.

В наше время мы все чаще и чаще используем технологии виртуальной реальности в повседневной жизни. Подобные технологии не могут пройти и мимо промышленной, научной отраслей хозяйства, в том числе и строительства.

Традиционное проектирование в основном работает с двумерными моделями объектов строительства. Они включают в себя чертежи, планы и остальную техническую документацию. Основное отличие BIM-проектирования – включая в себя данные об архитектурно-планировочных, конструктивных, экономических, технологических и эксплуатационных характеристиках объекта, оно позволяет воссоздать с максимальной точностью всю конструкцию в трехмерном изображении, которая также будет обладать реальными физическими свойствами.

Building Information Modeling (BIM) – в переводе на русский: информационное моделирование здания. Аббревиатура обозначает комплекс мероприятий и работ по управлению жизненным циклом здания, начиная от проекта и заканчивая демонтажем.