ISSN 2225-5435

# Вестник УрФО

## БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(11) / 2014



**Подписной индекс 73852 в каталоге «Почта России»**

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство **ПИ № ФС77-44941** от 05.05.2011

Издатель: ООО «Южно-Уральский юридический вестник»

Адрес редакции: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.

**Тел./факс: (351) 267-90-65, 267-97-01.**

Электронная версия журнала в Интернете: **www.info-secur.ru, e-mail: urvest@mail.ru**

# В НОМЕРЕ

## HISTORICAL ASPECT



## ENGINEERING AND TECHNICAL INFORMATION SECURITY



## CRYPTOGRAPHIC INFORMATION SECURITY



## PROGRAM AND HARDWARE INFORMATION SECURITY



## ORGANIZATIONAL INFORMATION SECURITY



## PERSONNEL TRAINING FOR THE SPHERE OF INFORMATION SECURITY



## TRIBUNE OF YOUNG SCIENTISTS



## THE PRACTICAL ASPECT

**Соколов А. Н.**

# ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ В СИСТЕМЕ ПОДГОТОВКИ КАДРОВ ДЛЯ СФЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНА

Зав. кафедрой «Безопасность информационных систем», канд. техн. наук, доцент
**Соколов Александр Николаевич**

*Уважаемые коллеги, читатели журнала «Вестник УрФО. Безопасность в информационной сфере»! От себя лично и от лица профессорско-преподавательского состава кафедры «Безопасность информационных систем» Южно-Уральского государственного университета (ЮУрГУ, г. Челябинск) рад приветствовать вас на страницах первого выпуска Вестника, материалы для которого полностью подготовлены студентами, аспирантами и преподавателями кафедры «Безопасность информационных систем», как молодыми, так и достаточно опытными. Это первый подобный опыт в рамках журнала, и, я надеюсь, он станет хорошей традицией для вузов Уральского федерального округа, которая позволит нам лучше узнать друг о друге.*

Кафедра «Безопасность информационных систем» (БИС) была образована 1 октября 2011 года на Приборостроительном факультете (компьютерных технологий, управления, радиоэлектроники) путем выделения из кафедры «Цифровые радиотехнические системы» (ЦРТС) направления подготовки бакалавров и специальностей укрупненной группы «Информационная безопасность». С 2012/13 учебного года две выпускающие кафедры ЮУрГУ — «Информационная безопасность» (существовала в ЮУрГУ с 1999 года) и «Безопасность информационных систем» — были объединены в составе кафедры «Безопасность информационных систем» приборостроительного факультета. Таким образом на одной кафедре удалось создать педагогический коллектив из опытных преподавателей университета по различным направлениям защиты информации.

В настоящее время кафедра ведет набор и осуществляет подготовку по следующим основным образовательным программам в рамках образовательных стандартов ФГОС-III и ГОС-II:

**БАКАЛАВРИАТ** (степень — академический бакалавр):

— 10.03.01 (090900) — «Информационная безопасность» (профили «Организация и технология защиты информации», «Безопасность автоматизированных систем», ФГОС-III);

**СПЕЦИАЛИТЕТ** (квалификация — специалист по защите информации):

— 10.05.03 (090303) — «Информационная безопасность автоматизированных систем» (специализация «Информационная безопас-

ность автоматизированных систем критически важных объектов», ФГОС-III);

— 10.05.05 (090915) — «Безопасность информационных технологий в правоохранительной сфере» (специализация «Информационно-аналитическое обеспечение правоохранительной деятельности», ФГОС-III);

— 090103 — «Организация и технологии защиты информации» (ГОС-II);

— 090104 — «Комплексная защита объектов информатизации» (ГОС-II);

— 090105 — «Комплексное обеспечение информационной безопасности автоматизированных систем» (ГОС-II).

На кафедре организовано 8 специализированных учебно-научных лабораторий:

1. Полигон технической защиты информации.
2. Аппаратные средства вычислительной техники.
3. Технологии обеспечения информационной безопасности объектов информатизации.
4. Управление информационной безопасностью.
5. Программно-аппаратные средства обеспечения информационной безопасности, технические средства и системы в защищённом исполнении.
6. Безопасность сетей ЭВМ и операционных систем.
7. Сетевые компьютерные и интернет-технологии.
8. Безопасность систем баз данных.

На кафедре открыта аспирантура по специальностям: 13.00.08 «Теория и методика профессионального образования» (научный руководитель — д. п. н., профессор Л. В. Астахова) и 05.13.19 «Методы и системы защиты информации, информационная безопасность» (научный руководитель — к. т. н., доцент А. Н. Соколов).

Основные направления научной деятельности кафедры:

• оптимизация процесса аттестационных испытаний объектов информатизации на соответствие требованиям безопасности информации, содержащей сведения ограниченного распространения;

• моделирование технических каналов утечки информации средств вычислительной техники и оптимизации методик инструментального контроля защищенности информации;

• программная интеграция криптопровайдеров в программное обеспечение для применения в электронном документообороте с использованием средств криптографической защиты информации;

• оптимизация и структуризация научной базы биометрических признаков контроля доступа;

• разработка технологий обеспечения информационно-психологической и кадровой безопасности как средств организационной защиты информации;

• разработка методик и автоматизация оценки кадровых уязвимостей информационной безопасности.

В 2013 году во исполнение Приказа Министерства образования и науки Российской Федерации от 9 марта 2005 года № 126 «Об утверждении Перечня региональных учебно-научных центров по проблемам информационной безопасности в системе высшей школы на базе государственных образовательных учреждений высшего профессионального образования, находящихся в ведении Федерального агентства по образованию» при кафедре «Безопасность информационных систем» был создан и успешно функционирует Региональный учебно-научный центр «Информационная безопасность» Южно-Уральского государственного университета. Центр осуществляет повышение квалификации и переподготовку кадров по проблемам информационной безопасности. Подробнее о программах Центра можно узнать в отдельных материалах нашего выпуска журнала.

Выпускники кафедры — специалисты по защите информации — успешно создают и поддерживают комплексные системы информационной безопасности на предприятиях, в организациях, учреждениях, разрабатывают технологии аудита и средств автоматизации при подготовке к аттестационным испытаниям, создают и совершенствуют системы кадровой безопасности. Высокий уровень теоретической и практической подготовки выпускников дает им широкие возможности карьерного роста. В настоящее время выпускники кафедры работают в органах государственной власти (в администрации губернатора Челябинской области, органах ФСБ, ФНС, МВД, министерствах, отделениях Пенсионного фонда, других государственных структурах), на предприятиях оборонно-промыш-

ленного комплекса, в российских и зарубежных банках, в бизнесе.

Кафедре «Безопасность информационных систем» удалось сохранить и приумножить традиции подготовки кадров в области защиты информации, которые уходят корнями в 80-е годы прошлого столетия, когда информационная безопасность стала одним из приоритетных направлений образовательной и научной деятельности ЮУрГУ.

Зав. кафедрой
«Информационная
безопасность»
докт. пед. наук, профессор
**Астахова Людмила Викторовна**

В 1987 году при ЧПИ (ЮУрГУ) был создан НИИ цифровых систем (НИИ ЦС), одной из задач которого было изучение процессов защиты информации от несанкционированного доступа в системах радионавигации. Кафедру «Цифровые радиотехнические системы» на приборостроительном факультете, как и сам НИИ ЦС, возглавил Юрий Трофимович Карманов — доктор технических наук, профессор, действительный член Российской академии естественных наук, Международной академии информатизации и Российской академии медико-технических наук. Однако отдельных специальностей по защите информации в советские годы не было.

В 1999 году на факультете экономики и права ЮУрГУ была создана кафедра «Информационная безопасность». Ее возглавила Людмила Викторовна Астахова — доктор педагогических наук, профессор, почетный работник высшего профессионального образования Российской Федерации, лауреат Национальной профессиональной премии в области информационной безопасности «Серебряный кинжал», выступившая инициатором открытия в Челябинской области специальностей группы «Информационная безопасность». В апреле 2002 года впервые в Челябинской области кафедра получила лицензию на образовательную деятельность по специальности «Организация и технология защиты информации». В апреле 2003 года впервые в Уральском федеральном округе (УрФО) на кафедре была открыта специальность «Комплексная защита объектов информатизации».

С первых лет своего существования кафедра была нацелена на отраслевой подход к информационной безопасности и явилась консолидирующим звеном в процессе профессионализации этой отрасли и ее инновационном становлении в Челябинской области.

В сентябре 2003 года на кафедре был создан Центр дополнительного профессионального образования. Решением Межведомственной комиссии по защите государственной тайны Российской Федерации (Решение № 95 от 06.04.2005) Южно-Уральский государственный университет был внесен в «Перечень учебных заведений, осуществляющих подготовку специалистов по вопросам защиты информации, составляющей государственную тайну, свидетельство об окончании которых дает руководителям предприятий,

Выпуск специалистов на кафедре
«Безопасность информационных систем» в 2013 г.

учреждений и организаций право на освобождение от государственной аттестации». Успешно началась работа курсов повышения квалификации кадров по защите государственной тайны. В 2006 году на базе ЦДПО кафедры был создан Центр защиты информации ЮУрГУ.

В процессе обучения студенты и слушатели получали всестороннюю подготовку в области информационной безопасности. Кафедра приложила много усилий, чтобы сделать обучение максимально практико-ориентированным, чутко реагируя на изменения потребностей рынка, работодателей, с которыми она поддерживает тесные контакты. Так, практику студенты кафедры проходят в силовых структурах (ФСБ, МВД), администрации Челябинской области и города Челябинска, в Представительстве Министерства иностранных дел России в Уральском федеральном округе, на Южно-Уральской железной дороге, в Южно-Уральской торгово-промышленной палате, в банках, на нефтегазовых и энергетических предприятиях и др.

Для адаптации к изменяющимся потребностям рынка труда были разработаны новые специализации. По инициативе кафедры и ее усилиями в 2001—2006 годы впервые в России были открыты специализации: «Конфиденциальное делопроизводство» (специальность 032001 «Документоведение и документационное обеспечение управления»), «Безопасность принятия управленческих решений» (специальность 090103 «Организация и технология защиты информации») и др.

Научно-технической базой обучения студентов являлись также инновационные площадки кафедры, к числу которых относятся УФНС по Челябинской области, а также лидеры рынка защиты информации в Челябинской области — компании-лицензиаты ФСБ и ФСТЭК «Стратегия безопасности», Межрегиональный консалтинговый центр «Аста-информ», «ПНК», «Энигма» и др. Эти организации и предприятия оказывали техническую и кадровую поддержку учебному процессу.

В 2006 году специальность 090104 «Комплексная защита объектов информатизации», открытая на кафедре «Информационная безопасность», и лаборатория инженерно-технической защиты информации были переданы на кафедру «Цифровые радиотехнические системы». На кафедре ЦРТС была открыта также специальность 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем». За кафедрой ЦРТС были закреплены дисциплины по техническим аспектам защиты информации, а за кафедрой «Информационная безопасность» — по организационно-управленческим, экономическим и информационно-психологическим проблемам. В 2007—2010 годы на кафедре ЦРТС по инициативе доктора физ.-мат. наук, профессора Александра Викторовича Рожкова проводилась ежегодная региональная олимпиада для школьников «Криптография и математика», официально поддержанная Институтом криптографии, связи и информатики Академии ФСБ.

В октябре 2002 года кафедра «Информационная безопасность» выступила организатором Международной научно-практической конференции «Региональная информационная экономика: проблемы формирования и развития», проведенной совместно с Правительством Челябинской области и Российским гуманитарным научным фондом (РГНФ) (проект № 02-02-00299 г/т).

В 2003 году кафедра совместно с ассоциацией предприятий оборонно-промышленного комплекса Челябинской области организовала Региональный научно-практический семинар «Система подготовки, переподготовки и повышения квалификации кадров по защите информации в Челябинской области», положивший начало формированию названной системы.

В октябре 2004 года совместно с Администрацией Челябинской области кафедра организовала и провела Первую Всероссийскую научно-практическую конференцию «Информационная безопасность региона», а в ноябре 2009 года проведена Вторая конференция.

С 2008 года кафедрой «Информационная безопасность» (а с 2013 года — кафедрой «Безопасность информационных систем») совместно с партнером МКЦ «АСТА-информ» ежегодно проводятся областные научно-практические конференции по защите персональных данных.

На кафедре была открыта аспирантура по специальностям: 13.00.08 «Теория и методика профессионального образования» (научный руководитель — д. п. н., профессор Л. В. Астахова) и 05.13.19 «Методы и системы защиты информации, информационная безопасность» (научный руководитель — к. т. н., доцент Ю. Н. Макаров). В ней обучались аспиранты, которые работали как над технически-

ми, так и над гуманитарными (психологическими, педагогическими, правовыми, социологическими) проблемами информационной безопасности. Под руководством доктора педагогических наук, профессора Л. В. Астаховой на кафедре сложилась научная школа по проблемам организационно-управленческой подготовки будущих специалистов по защите информации. По разным аспектам информационной и информационно-психологической безопасности под ее руководством защитили кандидатские диссертации 8 аспирантов и соискателей.

Аспиранты кафедры прошли курс обучения в Международной летней школе «Математические основы и технологии защиты информации» (ВМиК МГУ им М. В. Ломоносова), выиграли гранты губернатора Челябинской области на исследования проблем информационно-психологической безопасности и др.

Активное участие в научно-исследовательской работе всегда принимали студенты. С результатами исследований студенты выступали на университетских, всероссийских и региональных конференциях по информационной безопасности: Конференция молодых ученых (Санкт-Петербургский государственный университет информационных технологий, механики и оптики), «Перспектива» (Южный федеральный университет), «Информационная безопасность региона» (ЮУрГУ), «Безопасность информационного пространства» (УГТУ-УПИ, УрГУ, ЮУрГУ, ТГУ, УрФУ), ежегодная студенческая научно-практическая конференция ЮУрГУ и др.).

В мае 2011 года совместно с Координационным советом по подготовке, переподготовке и повышению квалификации кадров в Уральском федеральном округе кафедра выступила инициатором и организатором Первой Региональной интернет-конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства», в которой приняли участие все вузы УрФО, которые готовят специалистов по защите информации.

Ежегодно кафедра представляла ЮУрГУ на межрегиональных выставках «Информатика и связь. Средства защиты и безопасность» (Выставочный центр «Восточные Ворота») и «Формула безопасности. Системы связи и информационные технологии» (Региональный выставочный центр «ЮжУралЭкспо»), проводила в рамках этих выставок специализированные научно-практические семинары, за что не раз награждалась дипломами Правительства Челябинской области и администрации г. Челябинска. За большой вклад в подготовку специалистов по защите информации для Уральского региона профессор Л. В. Астахова награждена грамотами и благодарностями Министерства образования и науки Российской Федерации, Управления ФСТЭК по Уральскому федеральному округу, Управления ФСБ по Челябинской области, губернатора Челябинской области, ректора ЮУрГУ.

Большим событием и ответственным делом для Южно-Уральского государственного университета стало учреждение в 2011 году специального научного журнала «Вестник УрФО. Безопасность в информационной сфере». Издание Вестника было поручено ЮУрГУ Координационным советом по подготовке, переподготовке и повышению квалификации кадров в Уральском федеральном округе. Активное участие в подготовке материалов для журнала от ЮУрГУ принимают: проректор по учебной работе, докт. юрид. наук Владимир Иванович Майоров, Специальное управление (начальник Евгений Алексеевич Тряскин), юридический факультет (зам. декана докт. юрид. наук Алексей Владимирович Минбалеев), приборостроительный факультет (зам. декана, докт. пед. наук Людмила Викторовна Астахова, зав. каф. «Безопасность информационных систем» канд. техн. наук, доцент Александр Николаевич Соколов) и др.

Замечательной традицией, родившейся в 2004 году на кафедре «Информационная безопасность» и продолженной на кафедре «Безопасность информационных систем», стало проведение «Дня защиты информации на Приборостроительном», посвященного Международному дню защиты информации. Он отмечается 30 ноября во всех странах, начиная с 1988 г. На нем принято подводить итоги нашей работы, награждать победителей олимпиад, участников конференций, лучших студентов по результатам успеваемости, научной, общественной работы и т. д.

Обязательными участниками праздника бывают специалисты по защите информации — наши выпускники разных лет. Всего с 2007 года ЮУрГУ выпустил более 300 специалистов по защите информации. Все они верны своей профессии, поэтому приходят поделиться со студентами секретами своей успешной карьеры.


Студенты и сотрудники кафедры «Безопасность информационных систем»
на празднике, посвященном Международному дню защиты информации, 28 ноября 2013 г.

Подготовка, переподготовка и повышение квалификации кадров для сферы информационной безопасности региона является приоритетной задачей Южно-Уральского государственного университета. И кафедра «Безопасность информационных систем», на которую возложена эта ответственная миссия, будет и дальше прилагать все усилия для ее реализации.

---

**Кафедра «Безопасность информационных систем»**
**ФГБОУ ВПО «ЮУрГУ» (НИУ)**

**454080, г. Челябинск, пр. Ленина, 76**
**Тел.: 8 (351) 267-93-55, 267-99-24**

**E-mail: kbis-susu@mail.ru**
**Сайт: http://www.kbis.susu.ac.ru**

УДК 621.317.7 + 621.3/.6.08 + 621.396.67.08

**Антясов И. С., Войтович Н. И., Соколов А. Н.**

# ОСОБЕННОСТИ ВАЛИДАЦИИ АЛЬТЕРНАТИВНОЙ ИЗМЕРИТЕЛЬНОЙ ПЛОЩАДКИ ДЛЯ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ ТЕХНИЧЕСКИХ СРЕДСТВ

*В статье рассмотрены: проблемы построения и особенности валидации альтернативных измерительных площадок для проведения специальных исследований технических средств, возможности применения альтернативных измерительных площадок для проведения специальных проверок технических средств, проблемы выбора места размещения измерительной площадки и критерии оценки его эксплуатационной пригодности. Предложены решения, позволяющие оптимизировать технические мероприятия и экономические затраты на приведение альтернативной измерительной площадки в соответствие утвержденным нормативам. Приведены методики оценки затухания, эффективности экранирования и коэффициента стоячей волны по напряжению, позволяющие исследовать характеристики альтернативной измерительной площадки, влияющие на качество проведения не только специальных исследований, но и специальных проверок.*

***Ключевые слова:*** *антенна; вспомогательные технические средства и системы (ВТСС); измерительная площадка; канал утечки информации; побочные электромагнитные излучения и наводки (ПЭМИН); коэффициент стоячей волны по напряжению (КСВн); приёмник.*

**Antyasov I. S., Voytovich N. I., Sokolov A. N.**

# PECULIAR FEATURES OF VALIDATION OF ALTERNATIVE TEST SITES FOR CARRYING OUT ADVANCED TECHNICAL STUDIES OF TECHNICAL EQUIPMENT

*The article focuses on development and peculiar features of validation of alternative test sites for carrying out advanced technical studies of technical equipment, as well as the possibility of applying alternative test sites to specific inventories of technical equipment and*

*problems of location assignment for test sites and assessment criteria of their operational suitability. The author proposes solutions for optimization of technical measures and economic costs in the process of bringing alternative test sites into compliance with approved standards. The article also dwells on techniques of assessment of attenuation, screen effectiveness and voltage coefficient of standing wave receiver which allow to research the characteristics of alternative test sites affecting the quality of carrying out not only technical studies but also specific inventories.*

***Keywords:*** *antenna; supporting equipment and systems; test sites; covert channel; side electromagnetic radiation and pickups; voltage coefficient of standing wave receiver; technical studies.*

Неотъемлемой частью специальных исследований (СИ) являются поиск с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем (ВТСС), а также оценка соответствия защиты информации требованиям нормативных документов по защите информации. При проведении СИ требуются идеализированные условия распространения электромагнитной волны и отсутствие мешающих воздействий. Для этих целей используют специальные измерительные площадки[4], которые делятся на открытые и альтернативные (АИП)[1].

Необходимо заметить, что АИП могут применяться не только для СИ, но также и для мероприятий, связанных с проведением специальных проверок (СП). Например, проведение радиомониторинга технического средства (ТС) целесообразно проводить на специальных площадках, на которых мешающие воздействия сведены к минимуму. Также на АИП возможно проведение высокочастотного облучения для выявления параметрических закладок: так как закладные устройства могут переизлучать на частоте, отличной от частоты облучения, их обнаружение крайне затруднительно при наличии фоновых индустриальных помех. Соответственно, чтобы использовать АИП для проведения СП, их необходимо модернизировать — изменить рабочий частотный диапазон в соответствии с методиками. Следовательно, качественная АИП экономически выгодна организациям-лицензиатам, занимающимся одновременно проведением и СИ, и СП.

Существует ряд проблем, которые приводят к необходимости проведения абсолютного большинства СИ на АИП[1]. При построении АИП необходимо решить две наиболее сложные проблемы:

- экранирование от внешних электромагнитных излучений (ЭМИ);
- поглощение внутренних ЭМИ.

Пути решения проблем экранирования и поглощения ЭМИ противоположны друг другу: при усиленном экранировании возникает проблема стоячих волн внутри АИП, а при слабом экранировании внешние индустриальные помехи будут мешать проведению СИ.

Важнейшим этапом при построении АИП является выбор места её размещения. Однозначно оптимальным местом является подвальное помещение, расположенное как можно дальше от торцевых стен здания. Само помещение по возможности должно быть просторным, с высокими потолками. Целесообразность выбора помещения можно оценить по результатам предварительных измерений фоновых индустриальных помех. Предварительная оценка фоновых индустриальных помех позволяет значительно сэкономить средства для приведения площадки в соответствие с нормативно-методической документацией.

Оценка параметров затухания электромагнитных волн внутри АИП является обязательной при аттестации площадки. Параметры затухания должны соответствовать требованиям ГОСТа[4]. В соответствии с указанными требованиями, плоскость напольной части АИП должна быть ровной и свободной от каких-либо предметов, отражающих электромагнитные волны. При этом радиопоглощающее покрытие должно размещаться на расстоянии не менее 1 м от контура испытуемого ТС и антенны.

При аттестации измерительных площадок для проведения стендовых СИ испытуемых ТС особое место занимают измерение параметров затухания электрической составляющей электромагнитной волны на открытой (альтернативной) измерительной площадке и проверка отсутствия сверхнорма-

тивных отражений в соответствии с требованиями ГОСТа[4].

Измерение параметров затуханий электромагнитных волн на измерительной площадке проводится с целью проверки отсутствия сверхнормативных отражений в соответствии с требованиями ГОСТа[4]. Проверка осуществляется в диапазоне частот 30…1000 МГц. При этом экспериментально определяется напряжённость электрического поля тестового сигнала генератора в различных участках испытуемого объёма[1]. Конечное значение затухания рассчитывается как разность уровней напряжённости электрического поля, измеренного по схеме «б» (по кабелю) и схеме «а» (по полю) (рис. 1).

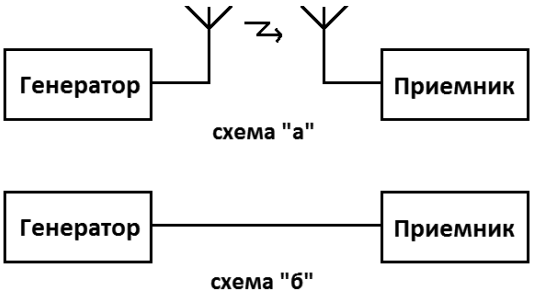


Рис. 1. Измерение параметров затуханий на АИП (а — по полю, б — по кабелю)

Оценка соответствия параметров затухания измерительной площадки определяется как разность между затуханием электромагнитных волн, полученным по результатам экспериментальных исследований на измерительной площадке, и нормированным затуханием электромагнитных волн на измерительной площадке, приведенным в ГОСТе[4]. По требованиям ГОСТа[4] полученная разность не должна превышать по модулю 4 дБ (рис. 2).

Поскольку стендовые СИ на ПЭМИН требуют проведения измерений на частотах свыше 1 ГГц, необходимо расширить ряд нормированных значений частот, на которых проводятся измерения затуханий при аттестации АИП, до значения 2 ГГц[1]. С этой целью проводится экстраполяция нормируемых значений затухания, с которыми сравниваются полученные экспериментальные данные (рис. 2).

ГОСТ[4] не поясняет, как именно должны размещаться передающая и приемная антенны относительно геометрии помещения АИП. В связи с этим возможны различные варианты расположения антенн относительно внутренних сторон АИП (рис. 3). Расположение антенн существенно влияет на значения затухания, получаемые экспериментальным путём. Как правило, при размещении антенн вдоль большей из сторон АИП полученные значения затухания наиболее близки к нормативным.

ГОСТ[4] не предъявляет обязательных требований к месту размещения измерительной аппаратуры и обслуживающего персонала.

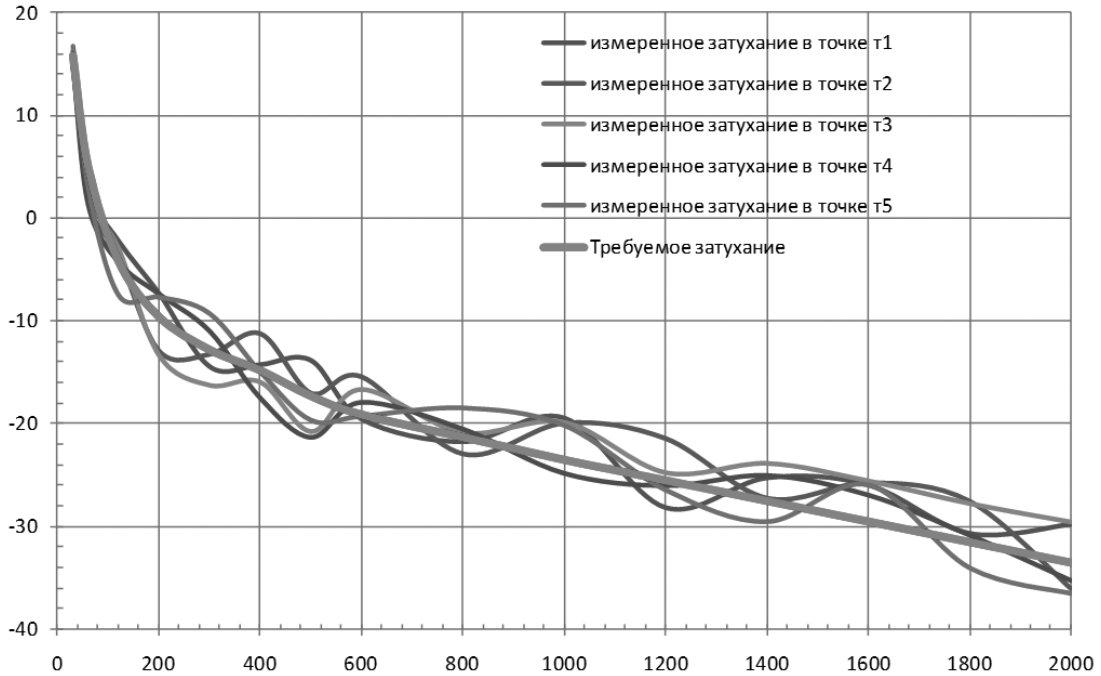


Рис. 2. Значения затухания для горизонтальной поляризации

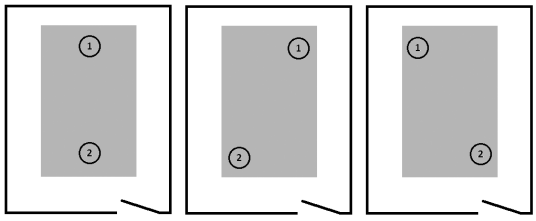

Рис. 3. Вариации расположения приемной и передающей антенн при испытаниях на затухания, где 1, 2 — места расположения антенн

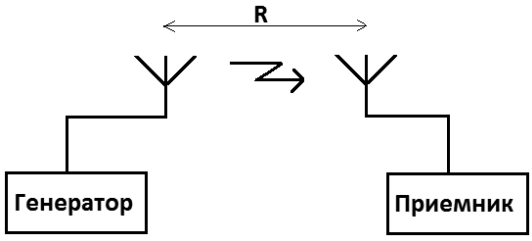


Рис. 4. Состав и размещение измерительной аппаратуры при контроле уровня излучаемого ЭМП при отсутствии экрана

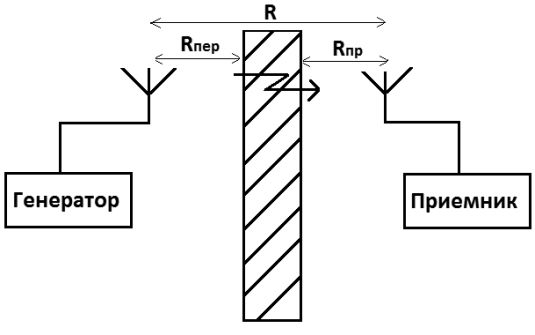


Рис. 5. Состав и размещение измерительной аппаратуры при контроле уровня излучаемого ЭМП, ослабленного экраном

Их размещение возможно как внутри АИП, так и за её пределами. Наличие внутри АИП измерительной аппаратуры и обслуживающего персонала оказывает существенное влияние на результаты измерений.

Для оценки влияния на результаты измерений установочного стола выполняются два измерения напряженности электрического поля: с использованием стола и без него (путём установки антенны на мачту такой же высоты). Оценка влияния установочного стола проводится в соответствии с требованиями ГОСТа[3].

ГОСТ[4] не предполагает исследования АИП на эффективность экранирования. Чем выше эффективность экранирования, тем ниже уровень фонового шума. Это позволяет точнее выделить информативный сигнал ТС и измерить его уровень. Испытания на эффективность экранирования проводят методом сравнения[2], который предполагает два последовательных измерения электромагнитного поля (ЭМП) — без экрана (рис. 4) и ослабленное экраном (рис. 5).

Измерения целесообразно проводить на контрольных точках в том же диапазоне частот (от 30 до 2000 МГц), что и при исследовании затуханий, для двух поляризаций: вертикальной и горизонтальной. В процессе измерений уровень выходного сигнала генератора на каждой частоте должен иметь постоянное значение.

Значение эффективности экранирования (в децибелах) вычисляется по формуле

$$Q=20\ \lg(E_1/E_2)= E_1(\text{дБ}) — E_2(\text{дБ}),$$

где $E_1$ — без применения экранирования, $E_2$ — с применением экранирования.

Значение эффективности экранирования позволяет оценить уровень промышленных шумов на АИП, что является важным фактором при проведении СИ. Измерения индустриальных шумов проводятся для магнитной и электрической составляющих электромагнитных волн в частотном диапазоне от 30 МГц до 2 ГГц. Всплески индустриальных помех существенно препятствуют проведению стендовых СИ как при обнаружении, так и при измерении уровня информативного сигнала от испытуемого ТС (рис. 6). Измерения уровня промышленных шумов проводятся несколько раз, в предполагаемое время проведения СИ на АИП. Результаты измерений подвергаются статистической обработке.

Поскольку планируемый диапазон измерений на АИП выше 1 ГГц, в соответствии с требованиями ГОСТа[3] на АИП необходимо проводить оценку коэффициента стоячей волны по напряжению (КСВн). Оценку КСВн проводят с целью выявления влияния переотражений ЭМИ от внутренних поверхностей АИП на испытания ТС произвольного размера и формы [3]. КСВн площадки оценивают в каждой позиции рабочего объема ТС для каждой поляризации путем последовательного проведения шести измерений вдоль линии, направленной на опорную точку приемной антенны. Критерием валидации при оценке КСВн является значение КСВн ≤ 6 дБ.

Таким образом, предложенные выше решения по построению АИП позволяют оптимизировать технические мероприятия и экономические затраты на приведение АИП в

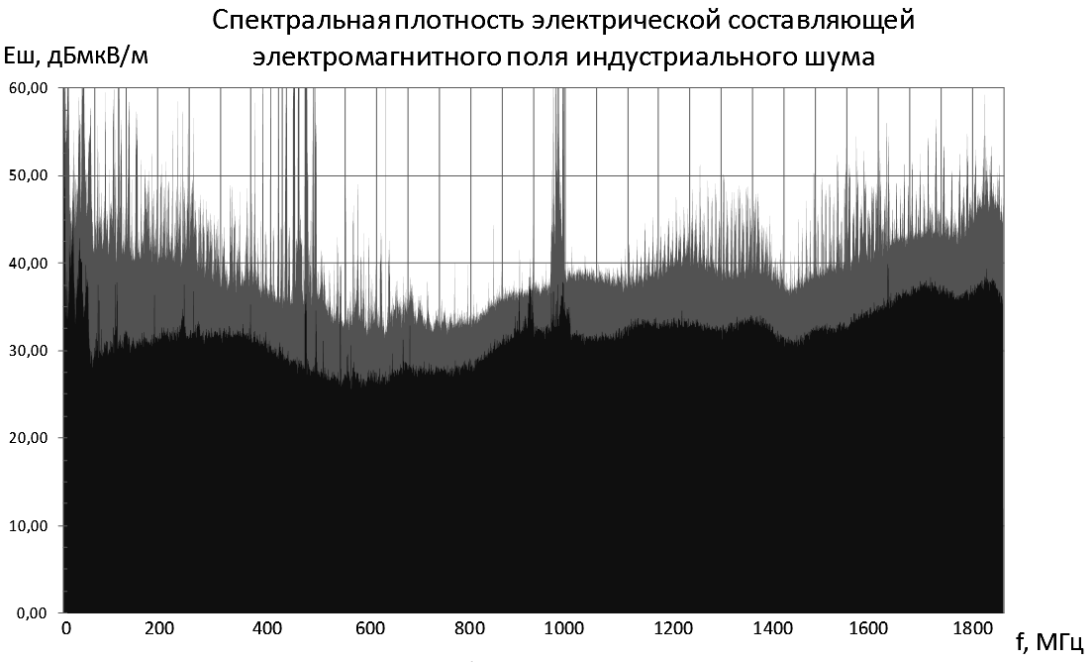


Рис. 6. Уровень фоновых индустриальных помех

соответствие утверждённым нормативам. Предложенные методики оценки затухания, эффективности экранирования и КСВн позволяют более полно исследовать характеристики АИП, которые влияют на качество проведения не только СИ, но и СП.

## Примечания

[1] Антясов, И. С. Анализ требований нормативно-технических документов к альтернативным измерительным площадкам для проведения специальных исследований технических средств / И. С. Антясов, И. С. Петров, А. Н. Соколов // Вестник УрФО. Безопасность в информационной сфере. — 2013. — № 1(7). — С. 4—9.

[2] ГОСТ Р 50414-92. Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний. — Введ. 1992-26-11. — М. : Госстандарт России, 1992. — 28 с.

[3] ГОСТ Р 51318.16.1.4-2008. Совместимость технических средств электромагнитная. Требования к аппаратуре для измерения параметров индустриальных радиопомех и помехоустойчивости и методы измерений. Часть 1—4. Аппаратура для измерения параметров индустриальных радиопомех и помехоустойчивости. Устройства для измерения излучаемых радиопомех и испытаний на устойчивость к излучаемым радиопомехам. — Введ. 2008-12-25. — М. : Госстандарт России, 2009. — 75 с.

[4] ГОСТ Р 51320-99. Радиопомехи индустриальные. Методы испытаний технических средств — источников индустриальных помех. — Введ. 1999-22-12. — М. : Госстандарт России, 1999. — 27 с.

## References

[1] Antyasov I. S., Petrov I. S., Sokolov A. N. Analiz trebovanii normativno-tekhnicheskikh dokumentov k al'ternativnym izmeritel'nym ploshchadkam dlya provedeniya spetsial'nykh issledovanii tekhnicheskikh sredstv [Analysis of requirements of normative and technical documents for alternative test sites for carrying out specific research of technical equipment]// Vestnik UrFO. Bezopasnost' v informatsionnoi sfere. — Chelyabinsk: Izd. tsentr YuUrGU Publ., 2013. — № 1(7) — p.4 – 9.

[2] All-Union State Standard P 50414-92. Electromagnetic compliance of technical equipment. Testing equipment. Screened chambers. Classification, basic parameters, requirements and methods of testing. – 1992-26-11. – Moscow: Russian State Standard, 1992. – 28 p. (In Russ.)

[3] All-Union State Standard P 51318.16.1.4-2008. Electromagnetic compliance of technical equipment. Equipment requirements for parameter measurement of radio interference and interference immunity; measuring methods. Part 1-4. Equipment for parameter measurement of radio interference and interference immunity. Equipment for measurement of radiated radio interference and radiation immunity test. 2008-12-25. – Moscow: Russian State Standard, 2009. – 75 p. (In Russ.)

[4] All-Union State Standard P 51320-99. Man-made noises. Testing methods of technical equipment, sources of man-made noises. 1999-22-12. – Moscow: Russian State Standard, 1999. – 27 p. (In Russ.)

**Антясов Иван Сергеевич,** специалист по защите информации Специального управления ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: antyasov@gmail.com

**Войтович Николай Иванович,** зав. кафедрой конструирования и производства радиоаппаратуры ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: VoytovichNI@mail.ru

**Соколов Александр Николаевич,** зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: ANSokolov@inbox.ru

**Ivan Sergeevich Antyasov,** security engineer of the special administration of the South Ural State University (National Research University)

**Nikolai Ivanovich Voitovich,** head of the Department of Radio Equipment Design and Production of the South Ural State University (National Research University)

**Aleksandr Nikolaevich Sokolov,** head of the Department of Information System Security of the South Ural State University (National Research University)

УДК 004.056.5 + 003.26:004.056
ББК Х401.114

**Животова А. Е., Зюляркина Н. Д., Костыгина Ю. О.**

# *МОДИФИКАЦИЯ КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ «ЗАДАЧИ О РЮКЗАКЕ»*

*В работе рассмотрены достоинства и недостатки криптосистем с открытым ключом, основой для которых является классическая формулировка «задачи о рюкзаке». Предложена идея модификации рюкзачной схемы, связанная с вычислениями в группах и использующая для построения рюкзака специально подобранные порождающие множества группы, которые обеспечивают однозначное представление заданного элемента. Приведен пример использования мультипликативного рюкзака, построенного при помощи прямого произведения диагональных подгрупп в общей линейной группе над конечным полем и замаскированного под рюкзак произвольного вида посредством внутреннего автоморфизма этой группы.*

***Ключевые слова:*** *криптосистема с открытым ключом, рюкзачная схема, группа, порождающий элемент.*

**Zhivotova A. E., Ziuliarkina N. D., Kostygina Y. O.**

# *MODIFICATION OF THE CRYPTOSYSTEM WITH PUBLIC KEY ON THE BASIS OF KNAPSACK PROBLEM*

*The article dwells on advantages and disadvantages of the cryptosystem with a public key based on the knapsack problem. The author proposes the idea of the modification of the knapsack scheme connected with the calculations in groups. For construction of a knapsack the scheme uses specifically matching groups which produce multitudes and provide single-valued representation of a stated element. The author gives an example of the usage of a multiplicative knapsack created with the help of direct product of diagonal subgroups of the general linear group over a finite field and disguised as a knapsack of general form by the inner automorphism of the group.*

***Keywords:*** *cryptosystem with public key, knapsack scheme, group, generating element.*

Начало асимметричным шифрам было положено в 1976 г. в работе У. Диффи и М. Хеллмана «Новые направления в современной криптографии»[1].

Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр) — система шифрования, при которой открытый ключ передаётся по открытому каналу и используется для шифрования сообщения. Для расшифровки сообщения используется секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах и стандартах цифровой подписи.

Для построения криптосистемы с открытым ключом выбирается класс задач, для которого в произвольном случае не известен эффективный алгоритм решения, и в этом классе выделяется подзадача, для которой такой алгоритм существует. Выбранную задачу маскируют под задачу общего вида и на основе ее выбирают ключ шифрования. В качестве секретного ключа используется информация, позволяющая перевести выбранную задачу в исходный вид.

Наиболее распространенными в настоящее время являются криптосистемы, основанные на задаче факторизации (RSA) и задаче нахождения дискретного логарифма (схема Эль-Гамаля). Но усовершенствование технических средств требует постоянного изменения параметров систем, основанных на задаче факторизации, что приводит к определенным сложностям при их использовании. Ввиду этого актуальность приобретают методы построения асимметричных криптосистем, которые не используют задачи, связанные с факторизацией. В связи с этим особенно активно изучаются способы, основанные на вычислениях в специально подобранных группах. Отметим в качестве примера группы точек эллиптических кривых, которые используются в обобщенной схеме Эль-Гамаля, применяемой в стандартах цифровой подписи. К достоинствам этих групп следует отнести наличие элементов большого порядка и сложность нахождения дискретного логарифма.

К задачам, не связанным с проблемой факторизации, относится и задача об укладке рюкзака, являющаяся NP-полной. На ее основе был разработан ряд криптосистем, отличающихся простотой реализации. Но в ходе их анализа были выявлены существенные недостатки, делающие эти системы уязвимыми для различного вида криптографических атак. В настоящее время системы этого класса не получили широкого распространения, но ведется работа по их модификации, которая позволит улучшить их надежность. Одним из способов такой модификации является использование специальных порождающих множеств в конечных группах для создания рюкзачной схемы.

## 1. Криптосистемы на основе задачи о рюкзаке

**Задача о рюкзаке.** Имеется упорядоченный набор чисел $(a_1,a_2,...a_n)$ (этот набор называют рюкзаком или рюкзачным вектором) и число m. Требуется указать такой бинарный вектор $(x_1,x_2,...x_n)$, для которого выполняется равенство

$$x_1 a_1+x_2 a_2+...+x_n a_n=m.$$

В общем случае для данной задачи нет эффективного алгоритма решения и приходится применять полный перебор для нахождения требуемого вектора или доказательства отсутствия решения. Кроме того, в общей постановке задача о рюкзаке может иметь несколько различных решений. Но если рюкзак является сверхрастущим, то решение в случае его существования единственно и существует эффективный алгоритм его нахождения.

Рюкзак с положительными элементами $(a_1, a_2, ..., a_n)$ будем называть сверхрастущим, если $a_2>a_1$, $a_3>a_j+a_2,...,a_n>a_1+a_2+...+a_{n-1}$.

На основе задачи о рюкзаке разработан ряд криптографических систем. Первой из них была система Меркля — Хеллмана, описание которой приведено ниже.

**Генерация ключей:**

1. Выбирается некоторый сверхрастущий рюкзак.
2. Выбирается число k ($k > a_1+a_2+\ldots+a_n$).
3. Выбирается число c, взаимно простое с k.
4. Формируется рюкзак-ловушка $(b_1,b_2,\ldots b_n)=c(a_1,a_2,\ldots a_n) \pmod k$, который и является открытым ключом.
5. Числа c и k являются секретными ключами.

**Алгоритм шифрования:**

1. Открытый текст представляется в виде двоичной последовательности.
2. Последовательность разбивается на блоки длины n.

3. Каждый блок $(x_1,x_2,\ldots x_n)$ заменяется на число m, вычисленное по правилу

$$\sum_{i=1}^{n} a_i x_i = m.$$

**Алгоритм дешифровки:**

1. Находится исходный сверхрастущий рюкзак:
   $(a_1,a_2,\ldots,a_n)=c^{-1}(b_1,b_2,\ldots b_n) \pmod k$.
2. Для каждого элемента m шифр текста вычисляется элемент $m'=c^{-1}m$.
3. Для вычисленного m' решается задача о рюкзаке для рюкзака $(a_1,a_2,\ldots,a_n)$ и находится блок открытого текста $(x_1,x_2,\ldots,x_n)$.

**Пример 1.** Используется латинский алфавит, в котором каждая буква представлена пятиразрядной двоичной записью своего номера. Рюкзак-ловушка B=(182, 128, 192, 175, 50, 100) получен из сверхрастущего рюкзака A путем умножения на c=91 и приведением по модулю n=300. Сообщение Y=(232, 178, 502) получено шифрованием на основе рюкзака B. Восстановить исходный рюкзак A и, используя его, расшифровать сообщение Y.

Решение:

1) Найдем $c^{-1} \pmod{300}$: $c^{-1}=91^{-1}=211$.

2) Восстановим исходный рюкзак: $A=211B \pmod{300} = 211(182, 128, 192, 175, 50, 100) \pmod{300} = (2, 8, 12, 25, 50, 100)$.

3) Преобразуем сообщение Y: $Y \rightarrow Z = 211Y \pmod{300} = 211(232, 178, 502) \pmod{300} = (52, 58, 22)$.

4) Решим задачу о рюкзаке для каждого элемента сообщения Z:

$$52=50+2 \rightarrow (1, 0, 0, 0, 1, 0),$$
$$58=50+8 \rightarrow (0, 1, 0, 0, 1, 0),$$
$$22=12+10=12+8+2 \rightarrow (1, 1, 1, 0, 0, 0).$$

5) Запишем полученные двоичные векторы в единую последовательность, которую разобьем на блоки длины 5: (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) → (1, 0, 0, 0, 1), (0, 0, 1, 0, 0), (1, 0, 1, 1, 1), (0, 0, 0). Последний блок из трех элементов исключим из рассмотрения.

6) Сопоставим каждому полученному блоку число, для которого этот блок является двоичной записью, и найдем соответствующую букву латинского алфавита:

$$(1, 0, 0, 0, 1) \rightarrow 17 \rightarrow R,$$
$$(0, 0, 1, 0, 0) \rightarrow 4 \rightarrow E,$$
$$(1, 0, 1, 1, 1) \rightarrow 23 \rightarrow X.$$

Кроме системы Меркля — Хеллмана отметим систему Грэма — Шамира, в которой также используется сверхрастущий рюкзак. Но маскировка его под рюкзак общего вида производится не с помощью приведения по модулю, а с использованием вектора случайного шума. В системе Мории — Касахары используется мультипликативный способ шифрования и формирования секретного ключа. Система Хора — Ривеста основана на вычислениях в конечных полях, а система Накаше — Штерна является гибридом системы Меркля — Хеллмана и алгоритма Полига — Хеллмана. Описание некоторых из этих схем можно найти в работе[2].

## 2. Модификация рюкзачных криптосистем с использованием конечных групп

Пусть G — группа, $g_1\ g_2, \ldots, g_n$ — её элементы, такие, что для любого вектора $(x_1, x_2, \ldots, x_n)$, $x_i \in Z_{mi}$, $m_i=|g_i|$ элемент $g=g_1^{x1}g_2^{x2}\ldots g_n^{xn}$ имеет единственное представление в указанном виде. Будем предполагать, что существует эффективный алгоритм, позволяющий по данному элементу g находить вектор $(x_1, x_2, \ldots, x_n)$, $x_i \in Z_{mi}$, $m_i=|g_i|$, для которого выполняется равенство $g=g_1^{x1}g_2^{x2}\ldots g_n^{xn}$. Тогда можно рассмотреть следующую рюкзачную криптосистему, основанную на вычислениях в данной группе G.

**Генерация ключей:**

1. Выбирается рюкзак $(g_1\ g_2, \ldots, g_n)$, для которого выполняются описанные ранее условия.
2. Выбирается маскирующий изоморфизм f из группы G в группу G'.
3. Формируется рюкзак-ловушка $(b_1,b_2,\ldots b_n)=(f(g_1), f(g_2),\ldots,f(g_n))$, который и является открытым ключом.
4. Отображение f является секретным ключом.

**Алгоритм шифрования:**

1. Открытый текст представляется в виде последовательности
   $(x_1, x_2, \ldots, x_n)$, $x_i \in Z_{mi}$, $m_i=|g_i|$.
2. Каждый блок $(x_1, x_2, \ldots, x_n)$ заменяется на элемент b, вычисленный по правилу: $b= b_1^{x1}b_2^{x2}\ldots b_n^{xn}$.

**Алгоритм дешифровки:**

1. Находится исходный рюкзак $(g_1,g_2,\ldots,g_n)=f^{-1}(b_1,b_2,\ldots,b_n)$.
2. Для элемента b шифр текста вычисляется элемент $g=f^{-1}(b)$. Для вычисленного g решается задача о рюкзаке для рюкзака $(g_1,g_2,\ldots,g_n)$ и находится блок открытого текста $(x_1,x_2,\ldots,x_n)$.

3. Для удобства вычислений элементы $g_1, g_2, \ldots, g_n$ можно выбрать так, чтобы они имели одинаковый порядок m. В этом случае исходный текст можно считать последовательностью элементов из $Z_m$ и при шифровании разбивать его на блоки длины n.

**Пример 2.** Рассмотрим общую линейную группу $G= GL_3(7)$ и выберем в ней элементы a, b и c:

$$a=\begin{pmatrix}3&0&0\\0&1&0\\0&0&1\end{pmatrix},\quad b=\begin{pmatrix}1&0&0\\0&5&0\\0&0&1\end{pmatrix},\quad c=\begin{pmatrix}1&0&0\\0&1&0\\0&0&3\end{pmatrix}.$$

Заметим, что <a, b, c> является прямым произведением подгрупп <a>, <b> и <c>, каждая из которых имеет порядок 6. Кроме того, по виду элемента $g=a^kb^sc^t$ набор (k, s, t) элементов из $Z_6$ легко восстанавливается. Следовательно, условия, накладываемые на элементы $g_1, g_2, \ldots, g_n$, будут выполняться.

В качестве маскирующего изоморфизма рассмотрим сопряжение посредством элемента x:

$$x=\begin{pmatrix}2&3&1\\1&4&2\\2&5&6\end{pmatrix}.$$ Заметим что $$x^{-1}=\begin{pmatrix}0&3&6\\1&2&5\\5&2&1\end{pmatrix}.$$

Вычислим набор $(a^x, b^x, c^x)$, который будет являться открытым ключом:

$$a^x=x^{-1}ax=\begin{pmatrix}1&0&0\\4&0&2\\6&2&4\end{pmatrix},\qquad b^x=x^{-1}bx=\begin{pmatrix}6&6&3\\1&5&2\\1&4&3\end{pmatrix},$$

$$c^x=x^{-1}cx=\begin{pmatrix}4&4&2\\6&2&4\\4&3&6\end{pmatrix}.$$

Зашифруем в данной системе сообщение (1, 5, 2):

$$(1,5,2)\longrightarrow b=a^x(b^x)^5(c^x)^2=\begin{pmatrix}5&5&6\\4&6&5\\5&2&4\end{pmatrix}.$$

Для дешифровки сообщения b найдем элемент g:

$$g=xbx^{-1}=\begin{pmatrix}3&0&0\\0&3&0\\0&0&2\end{pmatrix}.$$

Поскольку $3^1=3,\ 5^5=3,\ 3^2=2,\ g= a^1b^5c^2$ и открытый текст имеет вид (1, 5, 2).

Рассмотренная модификация опирается на мультипликативный рюкзак, поэтому представляется достаточно надежной ввиду того, что для подобных схем неизвестны эффективные способы взлома.

## Примечания


[1] Diffie, W. New Directions in Cryptography / W. Diffie, M. E. Hellman // IEEE Transactions on Information Theory. — 1977. — V. T. 1—22. — P. 644—654.

[2] Саломаа, А. Криптография с открытым ключом = Public-Key Cryptography / А. Саломаа. — Springer-Verlag, 1990. — С. 102—150.


## References


[1] Diffie W, Hellman M.E. New Directions in Cryptography. // IEEE Transactions on Information Theory ,V. TI-22,1977, pp 644-654.

[2] Salomaa A. Kriptografiya s otkrytym klyuchom [Public-Key Cryptography]. — Springer-Verlag Publ., 1990. — p. 102-150.



**Животова Анастасия Евгениевна,** студент кафедры «Безопасность информационных систем» Приборостроительного факультета ФГОБУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: nastiazhiv@mail.ru

**Зюляркина Наталья Дмитриевна,** кандидат физ.-мат. наук, доцент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: toddeath@yandex.ru

**Костыгина Юлия Олеговна,** студент кафедры «Безопасность информационных систем» Приборостроительного факультета ФГОБУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: kostygina250@mail.ru

**Anastasia Yevgenievna Zhivotova,** student of the Department of Information System Security of the Faculty of Instrument Design of the South Ural State University (National Research University). E-mail: nastiazhiv@mail.ru

**Natalia Dmitrievna Ziuliarkina,** cand. Sc. Physics and Mathematics, associated professor of Department of Information System Security of the South Ural State University (National Research University). E-mail: toddeath@yandex.ru

**Kostygina Yulia Olegovna,** student of the Department of Information System Security of the Faculty of Instrument Design of the South Ural State University (National Research University). E-mail: kostygina250@mail.ru

УДК 004.056.53 + 004.4.056

**Скурлаев С. В., Соколов А. Н.**

# ТЕХНИЧЕСКИЕ РЕШЕНИЯ, ПРИМЕНЯЕМЫЕ ДЛЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СИСТЕМАХ КЛАССОВ 3А И 2А

*Рассмотрены основные подходы к реализации механизмов защиты информации от несанкционированного доступа на примере некоторых средств защиты. Они идентичны друг другу или отличаются в зависимости от производителя. Выбраны наиболее распространенные реализации механизмов защиты и проанализированы взаимодействия соответствующих средств защиты с операционной системой и защищаемой информацией. Проведены исследования с применением продуктов Sysinternals: Autoruns, Process Explorer и Process Monitor. Показано, что все реализации обладают недостатками, которые можно компенсировать, применяя ручные настройки соответствующих служб операционной системы.*

***Ключевые слова:*** *автоматизированная система (АС), несанкционированный доступ (НСД), операционная система (ОС), средства вычислительной техники (СВТ), средство защиты информации (СЗИ).*

**Skurlaev S. V., Sokolov A. N.**

# TECHNICAL SOLUTIONS USED FOR 3A/2A CLASS SYSTEMS OF UNAUTHORIZED ACCESS PROTECTION

*The article discusses the main approaches to the implementation of typical technical solutions used for preventing unauthorized access to information. Certain approaches are identical to each other; others have differences depending on the manufacturer. Several most commonly used implementations were analyzed in terms of interaction with operating system and protected information. The following means of Windows Sysinternals products were used in research: Autoruns, Process Explorer and Process Monitor. It is shown that all approaches have its disadvantages which can be compensated using manual settings of appropriate operating system's services.*

***Keyword:*** *automated system (AS), unauthorized access (UA), operating system (OS), means of protecting information from unauthorized access.*

Основные положения по технической защите информации закреплены специальным нормативным актом Гостехкомиссии России «Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»[1]. В нём изложены цели и направления технической защиты информации в автоматизированных системах (АС) от несанкционированного доступа (НСД), а также основные способы обеспечения защиты. НСД определен как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или АС[1]. Концептуальные положения по технической защите информации (такие как классификация АС, модель нарушителя в АС, основные способы НСД и др.) раскрыты в других специальных нормативных актах. Классификация АС приведена в руководящем документе (РД) «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»[2]. В нём закреплены три основных класса АС, каждый из которых подразделяется на подклассы. К подклассам предъявляются определённые требования по реализации тех или иных механизмов. В связи с этим можно применять средства защиты, отвечающие требованиям, предъявляемым в ряде других специальных нормативных документов – РД Гостехкомиссии и ФСТЭК.

Довольно распространёнными АС являются системы 3-го и 2-го классов, с одним или несколькими пользователями соответственно, но обрабатываемая информация имеет одинаковый уровень ограничений к распространению. В то же время среди средств защиты информации (СЗИ) чаще встречаются такие, которые отвечают требованиям для АС классов 1Г (обработка несекретной информации) или 1Б (обработка до совершенно секретно включительно), потому что требования на более низкие классы выполняются автоматически. Но сами средства при этом весьма разнообразны, подходы разработчиков к реализации одних механизмов схожи, для других – отличны.

Для выполнения определённых требований все СЗИ используют системные функции операционных систем (ОС) семейства Microsoft Windows, например, дискреционную модель разделения доступа. Для выполнения других требований РД АС схожим остаётся только принцип функционирования. Соответственно, для реализации одних механизмов СЗИ сами предъявляют требования к системе, а для других – используют свои драйвера и службы. С целью узнать слабые и сильные стороны различных технических решений проведён эксперимент по изучению взаимодействия СЗИ с ОС.

Для эксперимента выбран следующий ряд СЗИ: Secret Net 6, СтражNT 3.0, Аура. Выбор основан на двух критериях: доступность экземпляра средства защиты для эксперимента и различие в технологических подходах к решению тех или иных задач. Эксперимент проведен с помощью программных продуктов от «Sysinternals» (Марк Руссинович, Брайс Когсвелл):

- Autoruns (отражает перечень драйверов, служб, модулей оболочки и входа в операционную систему и другое);
- Process Explorer (показывает работающие процессы, а также их подчинённость, используемые файлы и директории);
- Process Monitor (отслеживает действия всех процессов в системе, в том числе драйверов и библиотек, позволяет установить драйвер мониторинга с самого начала загрузки операционной системы).

С помощью этих программ проанализировано взаимодействие СЗИ с ОС, в том числе влияние на запросы ПО к защищаемой информации и устойчивость к сбоям.

**Secret Net 6** имеет сертификат соответствия требованиям РД СВТ[3] по 3 классу защищённости и РД НДВ[3] по 2 уровню. При выполнении технических условий применение этого средства возможно в подавляющем большинстве АС. Например, для ограничения загрузки с внешних носителей устанавливается плата аппаратной поддержки или электронный замок «Соболь» (в который можно установить считыватель идентификаторов iButton). При этом не исключается возможность использования других аппаратных идентификаторов, например eToken или Rutoken. Для функционирования требуются версии Professional операционных систем Windows от 2000 до 7, поскольку для управления средством требуются некоторые оснастки консоли (например, управление групповыми политиками).

В составе СЗИ имеются следующие компоненты:

- служба ядра;
- локальная база данных системы защиты;
- подсистема регистрации и журнал Secret Net;
- подсистема локального управления;
- защитные подсистемы;
- модуль входа;
- подсистема контроля целостности;
- подсистема работы с аппаратной поддержкой,

а также криптоядро, которое производителем не выделяется в отдельную компоненту, так как в нем применяются несертифицированные алгоритмы.

Некоторые из механизмов, включая драйвер ядра, работают как службы ОС. В случае отказа одной из служб перестают выполняться связанные с ней механизмы. Отказ службы драйвера ядра может привести к неработоспособности СЗИ в целом, позволяя зайти в систему только с административными правами. В случае использования СЗИ в АС третьего класса единственный пользователь будет иметь такие полномочия. В общем случае средство защиты расширяет возможности ОС, внедряя драйверы-фильтры в файловые операции, обращения к устройствам, подсистему входа-выхода и другие подсистемы. Настройки СЗИ хранятся в реестре и файле настроек СЗИ. При их повреждении не всегда остаётся возможной корректная деинсталляция средства защиты, что можно отнести к недостаткам Secret Net 6.

**СтражNT 3.0** имеет сертификат соответствия требованиям РД СВТ[3] по 3 классу защищённости и РД НДВ[4] по 2 уровню. Ограничение загрузки с внешних носителей реализовано путём сокрытия логической структуры диска – изменением информации в загрузочном секторе диска. В качестве аппаратных идентификаторов возможно применение различных устройств: гибких магнитных дисков, iButton, eToken, Rutoken и Guardant ID. СЗИ функционирует в любых версиях ОС Windows, начиная от 2000 и заканчивая 7.

СЗИ СтражNT 3.0 имеет следующие модули[5]:

- модуль входа в систему;
- модуль загрузки;
- модуль ядра системы защиты;
- службу доступа к устройствам;
- подсистемы защиты.

Ядро этого СЗИ реализовано как драйвер ядра ОС, поэтому вариант отказа средства защиты ввиду незапустившейся службы невозможен (все драйверы активны с момента загрузки ОС). Поскольку СЗИ при использовании модуля входа в систему обеспечивает сокрытие логической структуры диска, то слабым местом остаётся носитель-идентификатор: в случае утраты или неработоспособности вход в систему будет невозможен. Необходимо отметить, что само СЗИ при этом позволяет сделать дубликат идентификатора. Для разделения доступа так же, как и в Secret Net 6, используются драйверы-фильтры, которые перенаправляют запросы в случае обращений к файлам и устройствам внутренним механизмам СЗИ. Благодаря такому подходу данное средство является относительно независимым от ОС, под которой оно будет работать.

**Аура** имеет сертификат соответствия требованиям РД СВТ[3] по 3 классу защищённости и РД НДВ[4] по 2 уровню. Ограничение загрузки со сторонних носителей реализовано с помощью прозрачного преобразования дисков при помощи патентованных методов. В качестве аппаратных идентификаторов могут применяться Rutoken или iButton (для последнего необходимо использование электронного замка «Соболь»). ОС, поддерживаемые этим СЗИ, ограничены следующим перечнем: Microsoft Windows 2000 Professional SP4, 2000 Server SP4, XP Professional SP3, Server 2003 Standard Edition SP2, Server 2003 Enterprise Edition SP2, Server 2008 Standard Edition SP2, Server 2008 Enterprise Edition SP2, Vista Business SP2, Vista Ultimate SP2.

СЗИ имеет множество модулей, реализованных как в качестве службы, так и в качестве драйверов системы и библиотек оболочки. Примечательным является также механизм контроля целостности и редактирования базы данных пользователей, включая их полномочия, до загрузки операционной системы. Как и в случае с Secret Net 6, СЗИ поддерживает несертифицированное шифрование, но способно полностью преобразовывать диски, включая виртуальные, инструменты для создания которых имеются в самом СЗИ. Производитель отмечает следующие минусы своего продукта:

- отсутствие автоматизированной настройки мандатной системы разграничения доступа, что компенсируется выбором метки сессии (но сами метки можно устанавливать поверх файловой системы NTFS);

• отсутствие на данный момент возможности разделения доступа к конкретным устройствам, кроме накопителей (как правило, в большей части автоматизированных систем третьего и второго класса имеет лишь одно автоматизированное рабочее место, не включающее несколько различных устройств).

На данный момент слабым местом средства защиты информации является не очень широкий перечень поддерживаемых ОС.

Таблица 1 отражает основные подходы к реализации некоторых механизмов защиты, их достоинства и недостатки.

Таблица 1. Сравнение средств защиты информации

| **Средство защиты информации** | **Secret Net 6** | **Страж NT 3.0** | **Аура** |
|---|---|---|---|
| Ядро СЗИ | Служба и драйвер операционной системы | Драйвер ядра операционной системы | Отсутствует как таковое – служба операционной системы SKernel только обслуживает централизованную БД СЗИ |
| Механизмы контроля доступа к файлам | Реализованы как отдельные драйверы-фильтры операционной системы (запросы программ сравниваются с меткой сессии, объекта и разрешений пользователя) | Реализованы как отдельные драйверы-фильтры операционной системы | Реализованы как отдельные драйверы-фильтры операционной системы (запросы программ сравниваются с меткой сессии, объекта и разрешений пользователя), а также ряд служб, осуществляющих служебные операции |
| Ограничение загрузки | Аппаратный модуль (или программный для АС класса 1В) | Сокрытие логической структуры диска | Прозрачное преобразование (кодирование) дисков |
| Недостатки СЗИ | Слабым местом является служба ядра СЗИ, так как в случае отказа вход разрешается только администраторам. В случае отказа аппаратной части (хищения жёсткого диска с программным модулем ограничения загрузки) возможна загрузка со сторонних носителей | При контроле потоков не требуется выбирать уровень метки сессии, но значительно усложняется процесс настройки подсистемы мандатного доступа (для часто используемых программ есть шаблоны от производителя). В случае потери ключа преобразования загрузка ОС невозможна. Запросы программ перенаправляются механизмам СЗИ, поэтому для них логика их работы прозрачна, любая операция всегда завершается успешно, метка сессии не требуется. Широкий спектр поддерживаемых операционных систем | В случае отказа службы ядра СЗИ продолжает функционировать. В случае потери ключа шифрования загрузка операционной системы невозможна. Узкий перечень совместимых ОС |
| Достоинства СЗИ | Хорошая интегрируемость в операционную систему | Завершённость данного СЗИ – не требует дополнительных программных и аппаратных средств, кроме идентификаторов | Запуск данного СЗИ до загрузки ОС |

Таким образом, все СЗИ обладают как достоинствами, так и недостатками, наличие которых определяется используемыми технологиями и конкретными реализациями. Большую часть недостатков можно компенсировать, применяя ручные настройки соответствующих служб ОС. Например, проблема со службой ядра Secret Net 6 решается путём ручной настройки этой службы так, чтобы ОС сама перезапускала её. Все угрозы, связанные с потерей ключевых носителей, решаются путём создания резервной копии каждого из них с дальнейшим хранением этих копий в надёжном хранилище.

Таким образом, любые выявленные недостатки СЗИ можно устранить или уменьшить эффект их нежелательных последствий. Тем не менее выбор того или иного СЗИ должен определяться степенью риска потери защищаемых носителей или идентификаторов, а также утраты защищаемых данных во внештатных ситуациях.

## Примечания

[1] Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – Утверждено решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. — http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения 10.10.2013).

[2] Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. — http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения 10.10.2013).

[3] Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. — http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения 10.10.2013).

[4] Руководящий документ. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. – Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114. — http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения 10.10.2013).

[5] Система защиты информации от несанкционированного доступа «СТРАЖ NT». Версия 3.0. Описание применения. – 2010 г. — http://guardnt.ru/download/doc/app_guide_nt_3_0.pdf (дата обращения 10.10.2013).

## References

[1] Directive document. Concept of protection of hardware, computer equipment, and automated systems from unauthorized access. – Upheld by the State Presidential Technical Commission of the Russian Federation as of March 30, 1992. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (accessed 10.10.2013).

[2] Directive document. Automated systems. Protection from unauthorized access. Classification of automated systems and requirements on information protection. – Upheld by the State Presidential Technical Commission of the Russian Federation as of March 30, 1992. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (accessed 10.10.2013).

[3] Directive document. Hardware and computer equipment. Protection from unauthorized access. Index of protection from unauthorized access. – Upheld by the State Presidential Technical Commission of the Russian Federation as of March 30, 1992. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (accessed 10.10.2013).

[4] Directive document. Protection from unauthorized access. Part 1. Software of the means of information security. Classification on the basis of the level of control over the absence of undocumented features.. – Upheld by the State Presidential Technical Commission of the Russian Federation as of June 4, 1999. No. 114. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (accessed 10.10.2013).

[5] System of protection of information from unauthorized access «STRAZh NT» Version 3.0. – 2010 URL: http://guardnt.ru/download/doc/app_guide_nt_3_0.pdf (accessed 10.10.2013).

**Скурлаев Сергей Вадимович,** специалист по защите информации ООО «Стратегия безопасности». E-mail: sch1081024@mail.ru

**Соколов Александр Николаевич,** кандидат технических наук, доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: ANSokolov@inbox.ru

**Sergey Vadimovich Skurlaev,** security engineer of the LLC "Strategy of security". E-mail: sch1081024@mail.ru

**Aleksand Nikolaevich Sokolov,** cand. Sc. Engineering, associated professor, head of the Department of Information system Security of South Ural State University (National Research University). E-mail: ANSokolov@inbox.ru

УДК 342.7:004.056 + 347.15/.18 + 340.64:004.056
ББК Х401:114 + Х401.013

**Мищенко Е. Ю., Соколов А. Н.**

# *КОЛИЧЕСТВЕННЫЕ КРИТЕРИИ ИДЕНТИФИКАЦИИ ФИЗИЧЕСКОГО ЛИЦА ПРИ ОБЕЗЛИЧИВАНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ*

*Результатом обезличивания персональных данных является невозможность идентификации физического лица. Нормативные акты определяют некоторые критерии обезличивания, но все они, как правило, качественные. В статье проанализирована схема идентификации физического лица и дано обоснование применения не только качественных, но и количественных критериев обезличивания. Введены понятия вероятности идентификации и степени обезличивания персональных данных. Показано, что различные атрибуты персональных данных имеют разную значимость при идентификации, а количество атрибутов в группе-идентификаторе растет с ростом объема персональных данных.*

***Ключевые слова:*** *персональные данные, обезличивание персональных данных, вероятность идентификации, степень обезличивания.*

**Mishchenko E. Y., Sokolov A. N.**

# *QUANTITATIVE CRITERIA OF INDIVIDUAL IDENTIFICATION IN THE PROCESS OF DEPERSONALIZATION OF PERSONAL DATA*

*The result of depersonalization is the impossibility of the individual identification. Statutory acts define certain criteria of depersonalization, but all of them are generally qualitative. The article describes the scheme of individual identification and proves the application of not only qualitative but also quantitative criteria of depersonalization as well. The terms of identification probability and depersonalization degree are introduced. The article demonstrates that certain attributes of personal data have different effect on identification, and quantity of attributes in group identifier rises with the rise of personal data content.*

***Keywords:*** *personal data, depersonalization, identification probability, depersonalization degree.*

В статье «Обезличивание персональных данных: термины и определения»[1] проанализированы различные стороны процесса обработки персональных данных (ПД), их связь с такими субъектами, как Человек (физическое лицо, субъект обработки ПД), Оператор (уполномоченный — орган (или лицо), обрабатывающий или организующий обработку

ПД) и Контролер (федеральный орган исполнительной власти, контролирующий выполнение Закона[2]), рассмотрена терминология процесса обезличивания персональных данных. Показано, что процессы обезличивания и идентификации не могут быть описаны исключительно на качественном уровне.

Целью данной статьи является обоснование применения количественных критериев обезличивания ПД. Чтобы ответить на вопрос, является ли тот или иной набор информации обезличенными ПД, надо подтвердить эффективность обезличивания, то есть доказать, что некий показатель обезличивания изменился после проведения соответствующей процедуры в нужную сторону. Для этого введем понятие *вероятности идентификации* (ВИ) физического лица (ФЛ) в базе ПД — показателя, который в идеальном случае до обезличивания должен быть равен 1, а после обезличивания равен 0.

Значение ВИ = 1 для конкретного ФЛ означает, что его ПД однозначно сопоставлены ему в базе. Однако максимальное значение ВИ = 1 может быть достигнуто только в том случае, если в базе ФЛ нет абсолютно одинаковых, т. е. неразличимых с точки зрения возможностей идентификации. Фактически они могут быть — речь идет о физических близнецах (их около 2 %). И пока вопрос об их полной идентичности (по ДНК, отпечаткам пальцев) не решен, необходимо такую возможность учитывать для любой базы ПД.

Смысл значения ВИ = 0 сложнее для понимания. Фактически оно означает отсутствие возможности сопоставить ПД из базы некоторому ФЛ. При этом возможна ситуация, когда конкретному ФЛ можно сопоставить ПД нескольких «прочих» ФЛ. Чем больше «прочих» ФЛ, тем выше *эффективность обезличивания,* значение ВИ при этом обратно пропорционально количеству «прочих» ФЛ. Это означает, что идеальное значение ВИ = 0 недостижимо. В реальности необходимо требовать выполнения соотношения ВИ < НОРМ, где НОРМ — некое нормативное значение, обратное достаточно большому (тоже нормативному) количеству ФЛ, идентифицированных в обезличенном наборе вместо одного искомого ФЛ. Понятно, что максимальное количество ФЛ — это полное количество ФЛ в базе.

**1. Схема идентификации.** Нормативного определения термина «идентификация» не существует, поскольку его сущность определяется характеристиками всех сторон, принимающих участие в процессе идентификации. Кроме этого, идентификация решает две задачи: частную (принадлежат ли данные атрибуты заранее определенному ФЛ — «уточнение») и общую (какому именно ФЛ принадлежат данные атрибуты — «поиск»). При этом общая задача решается либо многократным повторением частного решения (перебор небольшого количества вариантов), либо поэтапным сужением области поиска с последующим перебором.

Рассмотрим схему взаимодействия сторон в процессе идентификации (рис. 1). На схеме представлены:

1) область поиска — набор информации, в рамках которого надо идентифицировать Человека (ПД). Для частной задачи — это ПД одного ФЛ, для общей задачи — это ПД некоторого количества ФЛ. Для области поиска как одной из сторон взаимодействия в про-

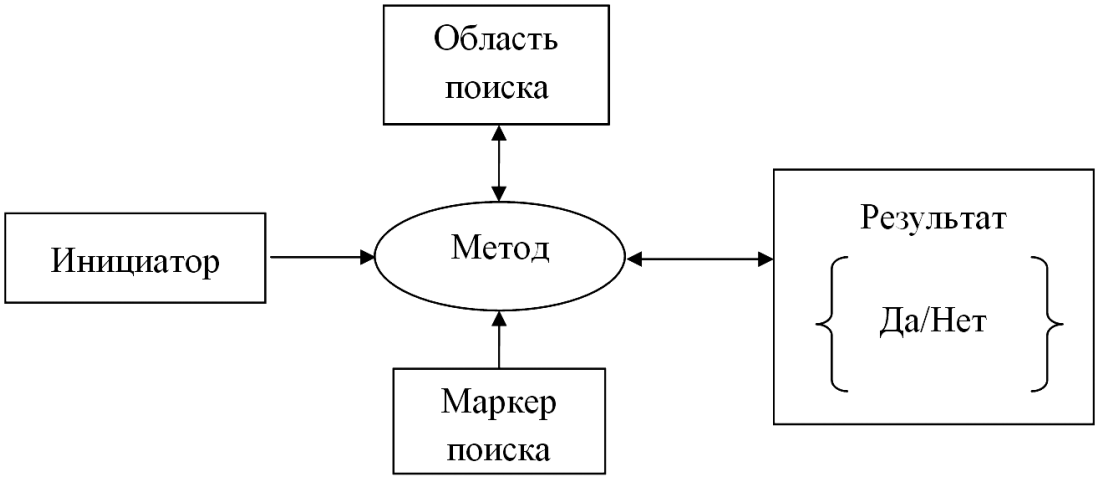


Рис. 1. Схема взаимодействия сторон в процессе идентификации

цессе идентификации можно ввести аналогию — базу данных (БД), где одна запись соответствует одному ФЛ, причем в этой записи заданы значения всех свойств из определенного набора атрибутов, т. е. пустых полей нет;

2) маркер поиска (МП) — набор информации об одном ФЛ (атрибуты неизвестного Человека, которого надо идентифицировать), причем заданы значения всех его атрибутов. Аналогия для МП — одна запись базы данных. МП задает цель поиска, а целью может быть идентификация группы ФЛ (например, все пациенты, больные диабетом), но для простоты в качестве цели поиска мы будем рассматривать ПД одного ФЛ;

3) инициатор процесса — является движущей силой идентификации. Им может быть кто угодно — от контролирующих органов до злоумышленников. У органов власти и силовых структур нет задачи проверки эффективности обезличивания ПД, т. к. они могут получить ПД официально. Проверка требуется только при проведении специальных испытаний, поэтому инициаторами, скорее всего, будут злоумышленники, не имеющие официального доступа к ПД;

4) метод идентификации — любой алгоритм идентификации, определяемый и применяемый инициатором, вне зависимости от достигаемого результата. Для частной задачи Метод представляет собой простое сравнение каждого атрибута, для общей задачи — должен учитывать Результат (двойная стрелка), который можно достигнуть путем нескольких итераций: при отрицательном результате изменяем область поиска (двойная стрелка) и продолжаем работу;

5) результат идентификации — может быть положительный или отрицательный. Для частной задачи он окончательный, для общей задачи — промежуточный, количество этапов при этом зависит от Метода.

**2. Взаимодействие Базы Данных и Маркера Поиска.** Маркер поиска взаимодействует с Базой Данных в рамках Метода. Идентификация — процесс поиска в БД всех записей о ФЛ, для которых значения всех атрибутов из МП (имеющихся в БД) совпадают с соответствующими значениями из БД. Сравнивать можно только те атрибуты МП, семантика которых совпадает с семантикой атрибутов БД (нет смысла сравнивать имя ФЛ с адресом проживания, но и адрес проживания с адресом деятельности тоже сравнивать бессмысленно). Для описания этого взаимодействия введем следующие количественные критерии:

1. Объем базы (ОБ) — количество записей в базе данных о ФЛ. Чем больше объем, тем меньше ВИ для имеющегося маркера поиска ФЛ (больше вероятность совпадений).

2. Количество атрибутов БД (КБ) — ассортимент свойств ФЛ в базе.

3. Количество атрибутов МП (КМ) — ассортимент свойств ФЛ в маркере. В общем случае КМ не равно КБ.

4. Количество атрибутов поиска (КП) — ассортимент свойств ФЛ, являющихся пересечением ассортимента БД и МП. В идеальном варианте все атрибуты МП входят в состав БД. В случае, когда КП меньше КМ, совокупность атрибутов поиска составляет набор поиска.

5. Атрибут АХ1, АХ2… — любое свойство (характеристика) ФЛ. Здесь и далее через Х обозначена принадлежность атрибута либо базе (АБ1, АБ2…), либо маркеру (АМ1, АМ2…), либо набору поиска (АН1, АН2…), а цифрой — порядковый номер атрибута. Аналогия — поле базы данных.

6. Название атрибута — НХ1, НХ2… в базе данных (НБ1, НБ2…) и в маркере (НМ1, НМ2…) или в наборе поиска (НН1, НН2…) отражает его семантику.

7. Значение атрибута АХ (ЗХ) — некая величина, соответствующая его семантике. Значение удобно обозначить аналогично названию атрибута (ЗХ1, ЗХ2…), а различные значения одного атрибута — ЗХ1-1, ЗХ1-2, ... .

8. Диапазон значений атрибута ЗХ1 — множество его значений, имеющее верхнюю (ЗХ1макс) и нижнюю (ЗХ1мин) границы. Значение атрибута может не иметь количественной семантики (семейное положение — холост / женат), в этом случае оно будет задано перечислением (ЗХ1-1, ЗХ1-2, …). Здесь и далее последняя цифра — номер варианта значения. Количество вариантов значений — от одного до полного количества записей ОБ.

9. Количество записей, имеющих атрибут с данным вариантом значения (КЗХ1-1), совпадает с количеством записей, найденных в процессе идентификации по конкретному атрибуту. Если для идентификации используется несколько атрибутов, то данная характеристика будет интегральной, и гораздо удобней использовать обозначение КИ. Нижней границей является КИ = 0 (ни одной записи не найдено). Теоретически это означает, что неправильно выбрана БД — в идеале Инициа-

тор должен быть априори уверен в успехе, но на практике при решении общей задачи это не так. В этом случае идентификация считается неуспешной (и это может быть признано решением задачи). Верхней границей является значение КИ = 1 (найдена ровно одна запись) — идентификация считается успешной. Если найдено несколько записей (КИ > 1) — идентификация считается условной.

10. Вес значения — отношение количества ФЛ, имеющих атрибут с данным вариантом значения, к общему количеству ФЛ в базе (ВЗХ1-1 = КЗХ1-1 / ОБ).

11. *Вероятность идентификации* (ВИ) — величина, обратная количеству найденных записей (ВИ = 1 / КИ). Отметим, что ВИ может не только рассчитываться как интегральная характеристика для всех атрибутов НП, но и определяться для каждого атрибута НП отдельно (ВИ1, ВИ2, …).

12. *Степень обезличивания* (СО) — интегральная характеристика базы ПД, являющаяся дополнением максимальной вероятности идентификации до единицы (СО = 1 — ВИ-макс) для некоторого достаточно большого (нормативного) количества операций идентификации (КСО). Если хотя бы в одном случае ВИ = 1 (успешная идентификация), то СО = 0. Очевидно, что КСО зависит от размера базы ОБ. Для оценки обезличивания также целесообразно ввести соответствующее нормативное значение СОнорм.

Проанализируем количественную зависимость значений ВИ и КИ от всех прочих критериев.

**2.1. Зависимость от объема базы ПД.** Объем базы (ОБ) определяется ее функциональным назначением и масштабом. От функционального назначения зависит количество записей об одном ФЛ, содержащихся в базе. Масштаб определяется количеством различных ФЛ в базе. Конечно, реальные базы ПД содержат не одну запись о конкретном ФЛ, а несколько (например, БД посещений поликлиники пациентами), но для простоты и ужесточения условий идентификации мы здесь будем рассматривать только БД-справочники, где одному реальному ФЛ соответствует ровно одна запись. Для данного случая ВИмин=1/ОБ и определяющее влияние на ВИ будет иметь масштаб. При определении масштаба надо учесть один нюанс — в базе могут содержаться ПД умерших людей — они тоже должны защищаться в соответствии с законом[2]. Если считать, что ПД умерших ФЛ не удаляются из базы, то значение ОБ увеличивается ежегодно в среднем на 1 % в соответствии с ростом рождаемости.

БД по масштабу можно классифицировать следующим образом:

1. Масштаб всей планеты — в мире живет около 7 миллиардов человек. Минимальная ВИ (для живущих) будет равна 1/7000000000. Это значение хоть и мало, но все-таки больше 0.

2. В масштабе нашей страны (даже с учетом умерших) ОБ можно принять равным 200 млн, в регионе — 10 млн, в районном центре — 100 тыс. и т. д. Поэтому минимальное значение ВИ в базе ПД небольшого предприятия будет, например, 1/100 или 1/20. Возникает вопрос: имеет ли смысл обезличивать такие маленькие базы? Ответом на него будет принятое нормативное значение ВИ.

**2.2. Зависимость от количества атрибутов.** В общем случае количество атрибутов базы КБ превышает их количество в Маркере КМ. Сравнение количества не имеет смысла, если не установлено соответствие семантики атрибутов БД и МП (при этом не ясно, что и с чем сравнивать). И хотя эта проблема относится не к количеству, а к значениям атрибутов, будем считать, что это соответствие установлено (т. е. количество атрибутов поиска КП определено).

ВИ слабо зависит от количества атрибутов и гораздо сильнее зависит от их значений. При прочих равных условиях чем меньше отношение КМ к КБ, тем меньше ВИ.

**2.3. Зависимость от значения атрибута.** Значение атрибута является решающим критерием для идентификации. В зависимости от семантики оно может иметь дискретный или непрерывный характер, но фактически, как правило, дискретный (существует определенный шаг, или точность значения, например, целесообразный шаг для роста — 10 см, для веса — 5 кг).

Количество возможных вариантов значений кроме шага определяется еще и диапазоном. Чем больше диапазон значения атрибута, тем больше ВИ с использованием этого атрибута.

На простом примере продемонстрируем упрощенный расчет ВИ (без учета веса значений) по таким атрибутам, как рост (диапазон — от 120 см до 200 см, 9 вариантов значений) и вес (диапазон — от 40 кг до 120 кг, 17 вариантов значений) человека. В нашем случае название атрибутов НН1 = НБ1 = «рост», НН2 = НБ2 = «вес». Ищем ФЛ со значениями ЗН1 =

170 см, ЗН2 = 90 кг. Значения атрибутов в базе ЗБ1-1 = 120 см, …, ЗБ1-9 = 200 см; ЗБ2-1 = 40 кг, …, ЗБ2-17 = 120 кг. В базе объемом ОБ = 1000 при равном весе значений будет найдено: записей ФЛ КЗБ1-6 = 1000 / 9 = 111 (ВИ1 = 1/111); записей ФЛ КЗБ2-11 = 1000 / 17 = 59 (ВИ2 = 1/59). Таким образом, по весу идентифицировать человека проще, чем по росту.

Показанный расчет является упрощенным, поскольку различные варианты значений атрибута встречаются в базе с разной вероятностью (вес значений различен), что оказывает значительное влияние на ВИ. В идеальном случае для определения ВЗ атрибута в БД должна быть рассчитана функция распределения значений по этому атрибуту. Чем меньше ВЗ, тем больше ВИ с использованием данного значения этого атрибута.

Продемонстрируем вышесказанное на следующем примере. Опыт говорит нам, что людей с ростом 170 см гораздо больше (это средний рост взрослого человека — максимум кривой распределения, ВЗБ1-6 = 25%), чем с ростом 200 см (ВЗБ1-9 = 1%). Соответственно, количество найденных в базе записей: КЗБ1-6 = 1000 · 0,25 = 250 (ВИ1-6 = 1/250); КЗБ1-9 = 1000 · 0,01 = 10 (ВИ1-9 = 1/10). Таким образом, ФЛ с ростом 170 см идентифицировать гораздо труднее, чем с ростом 200 см. С другой стороны, можно сделать вывод, что использование атрибута «рост» для идентификации в целом неэффективно. Эффективным будет использование атрибута, имеющего уникальное значение, при этом ВЗБ5-уник = 1 / ОБ, ВИ5-уник = 1. Если у атрибута все варианты значений уникальные, то этот атрибут полностью идентифицирует ФЛ, т. е. является *идентификатором*. Выявить такие атрибуты в базе очень важно, так как процедура идентификации обязательно будет на них опираться, а процедура обезличивания должна их нейтрализовать.

Таким образом, различные атрибуты имеют разную значимость при идентификации. По этому критерию атрибуты можно предварительно разделить на значимые и незначимые. В группу значимых войдут атрибуты, имеющие постоянные значения на протяжении длительных периодов жизни ФЛ (несколько лет, а в идеале — всю жизнь), имеющие дискретные значения из достаточно большого набора. Например, в эту группу не войдут: рост ФЛ (меняется со временем, большой вес значений), семейное положение (малый диапазон значений с большим весом: «холост / женат / разведен / вдовец»). Сложнее обстоят дела с атрибутом «место проживания» — его значение не всегда документально привязано к Человеку и может отличаться от указанного в документах. Вот серьезные кандидаты на включение в группу значимых: ДНК-анализ, отпечаток пальца, фотография (лицо), фамилия, имя, отчество, дата рождения, место рождения.

К сожалению, ни один из указанных значимых атрибутов в отдельности идентификатором быть не может. Принципиально не меняются только дата и место рождения ФЛ, т. е. для данного места ВИ определяется ежедневной рождаемостью. Но даже в небольшом населенном пункте со средней рождаемостью 1 человек в день вероятность рождения 2-х человек в один день достаточно высока, а в городе с населением 1 млн ежедневно рождается около 50 человек. Атрибуты ФИО и адрес хоть и не часто, но меняются, образ лица меняется постоянно, а у анализа ДНК и отпечатка пальца наибольший вес имеет значение «нет данных» (пример: в нашей стране есть федеральная база ДНК преступников, хотя в Исландии она включает всех жителей).

Все остальные атрибуты, входящие в состав ПД, будут либо незначимыми (нужны для целей обработки, но имеют большой вес значений — т. е. дополнительные сведения, ради которых ИСПДн существует, например, профессия ФЛ), либо косвенно значимыми (для целей обработки они не нужны, поэтому в явном виде отсутствуют, но могут оказывать значительное влияние на идентификацию — например, название предприятия отсутствует в базе данных отдела кадров, но фактически сильно ограничивает набор ПД и резко увеличивает ВИ).

Можно использовать в качестве идентификатора совокупность нескольких значимых атрибутов, но сначала рассмотрим еще одну группу — это такие атрибуты, как ИНН и номер паспорта. Мы не включили их в группу значимых, хотя это общепринятые идентификаторы во многих государствах мира. К упомянутым атрибутам можно добавить номер полиса медицинского страхования, водительского удостоверения, телефона, банковского счета… Проблема заключается в том, что все эти атрибуты не имеют прямого отношения к ФЛ, а являются искусственными ведомственными идентификаторами. По первоначальному замыслу все значения этих атрибутов уникальны, но реально это не так. Вот

причины, не позволяющие принять данные атрибуты в качестве идентификаторов:

1. Ограниченное распространение среди физических лиц (многих атрибутов нет у детей в принципе — в отличие от анализа ДНК, который можно взять у любого ФЛ).

2. Изменяемость значений (номера меняются в связи с утерей документов, сменой места жительства, просто по желанию ФЛ, т. е. не являются уникальными в отличие от некоторых значимых атрибутов).

3. Узковедомственная принадлежность (за рамками ведомственных реестров ограниченного доступа эти атрибуты не имеют смысла — попробуйте идентифицировать иностранца по номеру паспорта — т. е. не являются общепризнанными в отличие от значимых атрибутов).

Указанные причины позволяют признать данные атрибуты лишь условно значимыми, или служебными, т. е. каждый из них будет идентификатором ФЛ только при наличии доступа к соответствующему ведомственному реестру. В принципе каждый Оператор может составить свой реестр ПД и присвоить каждому ФЛ уникальный искусственный идентификатор в этом реестре.

Подводя итог, можно сказать, что в качестве идентификатора целесообразно выбирать совокупность значимых атрибутов. Чтобы определить, какие именно атрибуты использовать, необходимо для каждой из возможных групп рассчитать интегральную вероятность идентификации (ВИ). Группа с ВИ = 1 и будет идентификатором.

В качестве примера определим группу идентификаторов ФЛ для города с населением 1 млн человек. Будем принимать в расчет самые трудные варианты. Для атрибута «фамилия» ВИ будет больше, чем 1/100 (с учетом того, что женская фамилия отличается от мужской). Для атрибута «дата рождения» ВИ будет больше, чем 1/50 (365дн · 60 лет / 1 млн). А вот группа из этих двух атрибутов будет иметь ВИ = 1 (это идентификатор). Понятно, что расчет достаточно грубый. Для большей точности необходимо учитывать весовые коэффициенты каждой фамилии и каждой даты рождения в общем наборе информации (объем ПД). Но на конечный результат это вряд ли повлияет.

Не следует забывать и об объеме ПД — для крупного мегаполиса, например с 10 млн жителей, рассмотренная группа атрибутов даст лишь значение ВИ = 1/5. Но если в группу атрибутов добавить либо «имя», либо «инициалы», то этого будет достаточно даже для него.

Если рассматривать объем ПД масштаба страны, в описанную группу атрибутов придется еще добавить, например, «место рождения» и т. д.

Таким образом, количество атрибутов в группе-идентификаторе растет с ростом объема ПД. Подводит данную группу только возможная смена фамилии ФЛ, о которой Инициатор процесса может не знать. В этом случае результат идентификации будет отрицательный (ФЛ не найдено), а ВИ = 0. Поскольку Закон [2] требует подлинности ПД (за это отвечает Оператор) и очевидно, что в рассматриваемом случае база ПД устарела, значение ВИ = 0 должно означать законную (подлинную) смену значения одного из атрибутов группы-идентификатора. Поскольку для «даты рождения» такой процедуры нет, это будет означать, что изменилась «фамилия», и необходимы дополнительные сведения.

Возвращаясь к теме статьи и учитывая сказанное выше, можно сделать вывод, что смена фамилии — один из способов обезличивания ПД Человека, хотя и недостаточно эффективный. Следует отметить, что анализ различных методов обезличивания [3] и методов идентификации (как способа контроля степени обезличивания) выходят за рамки данной работы.

**Примечания**

[1] Мищенко, Е. Ю. Обезличивание персональных данных: термины и определения / Е. Ю. Мищенко, А. Н. Соколов // Вестник УрФО. Безопасность в информационной сфере. — 2013. — № 1(7) — С. 10—13.

[2] О персональных данных : Федеральный закон Российской Федерации от 27 июля 2006 № 152 (в редакции 2011 года). — http://www.garant.ru.

[3] Об утверждении требований и методов по обезличиванию персональных данных : приказ Роскомнадзора от 5.09.2013 г. № 996. — http://www.garant.ru.

**References**

[1] Mishchenko E.Yu., Sokolov A.N. Obezlichivanie personal'nykh dannykh: terminy i opredeleniya [Depersonalization of personal data]// Vestnik UrFO. Bezopasnost' v informatsionnoi sfere. — Chelyabinsk: Izd. tsentr YuUrGU Publ., 2013. — No. 1(7) — p.10 – 13.

[2] Federal law of the Russian Federation as of July 27, 2006 No. 152 «On personal data» (editorship as of 2011) [Electronic resource]. URL: http://www.garant.ru

[3] Order of the Federal Supervision Agency for Information Technologies and Communications as of 5.09.2013 No. 996 «On the establishment of regulations and methods on depersonalization of personal data» [Electronic resource]. URL: http://www.garant.ru

**Мищенко Евгений Юрьевич,** старший преподаватель кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: Eug6303@mail.ru

**Соколов Александр Николаевич,** заведующий кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: ANSokolov@inbox.ru

**Evgeny Yurievich Mishchenko,** senior lecturer and tutor of the Department of Information System Security of South Ural State University (National Research University). E-mail: Eug6303@mail.ru

**Aleksandr Nikolaevich Sokolov,** head of the Department of Information system Security of South Ural State University (National Research University). E-mail: ANSokolov@inbox.ru

УДК 004.4.056 + 005.953.2.004.056
ББК У9(2)248

**Астахова Л. В., Землянская О. О., Ефремов В. А.**

# АВТОМАТИЗАЦИЯ ОЦЕНКИ КАНДИДАТА НА ВАКАНТНУЮ ДОЛЖНОСТЬ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

*Вопросу анализа защищенности программно-технической составляющей информационных систем посвящено немало внимания, в то время как анализ защищённости пользователей информационных систем, т. е. кадровых уязвимостей информационной безопасности, находится на ранней стадии исследования. В статье охарактеризован созданный на основе авторской методики программный продукт «UVIS», позволяющий автоматизировать процесс оценки кандидата на вакантную должность в контексте информационной безопасности, описаны функциональные возможности его версий для оценщика и оцениваемого, а также проблемы его реализации. Особое внимание уделено уровню квалификации сотрудника, использующего программный продукт.*

***Ключевые слова:*** *оценка, уязвимость, кадровая безопасность, кандидат, информационная безопасность, автоматизация, программный продукт.*

**Astakhova L. V., Zemlianskaya O. O., Efremov V. A.**

# AUTOMATIZATION OF THE ASSESSMENT OF A CANDIDATE FOR A VACANT POSITION OF ENSURING INFORMATION SECURITY IN THE ORGANIZATION

*A great deal of attention is paid to the matter of protection of program and technical components of information systems while the analysis of protection of users of information systems (namely personnel vulnerability of information security) is on the earliest stage of its development. The article characterizes the software solution 'UVIS' based on unique method-*

*ology developed by the author. 'UVIS' allows automatization of the process of assessment of a candidate for a vacant position of ensuring information security in the organization, as well as the functional resources and opportunities of its versions for the assessor and the assesse, and problems of its implementation. Much attention is also paid to the level of qualification of the employee who uses the software.*

***Keywords:*** *assessment, vulnerability, personnel security, candidate, information security, automatization, software solution.*

Все методы оценки «человеческого капитала» возникают из потребности в его измерении и контроле. Сложность создания таких методов заключается в сложности объекта измерения. Чтобы измерение стало возможным, человека нужно охарактеризовать с помощью объективных количественных параметров, которые возможны только для материальных объектов. Однако попытки автоматизировать этот процесс предпринимаются в современной науке и практике. Так, специалисты СПИИРАН разрабатывают методы поиска вероятности успеха социоинженерного атакующего воздействия на пользователей информационной системы[1]. В их работах выявляются также взаимосвязи между психологическими особенностями, уязвимостями и возможными действиями пользователя информационной системы в рамках понятия социоинженерных атак[4]. Между тем, необходима методика перехода от исследований профиля психологических особенностей пользователя к профилю кадровых уязвимостей всех пользователей информационной системы в целом[2].

Созданная нами методика оценки кандидата[3] предназначена для использования при приеме сотрудника на работу. Оценка кандидата складывается из результатов собеседования, тестирования на осведомленность в вопросах информационной безопасности и поиска информации о кандидате в Интернете. Результатом являются процентный показатель уязвимости кандидата: от 0 % (кандидат уязвим с точки зрения информационной безопасности) до 100 % (кандидат неуязвим), а также графическое представление в виде диаграммы, разбитой по блокам. С целью автоматизации процесса оценки кандидата на вакантную должность нами создан программный продукт «UVIS v1.0».

Разработанный нами программный продукт является гибким, функциональным, учитывает специфику каждого структурного подразделения и степень конфиденциальности информации, с которой необходимо работать потенциальному сотруднику, и имеет дружественный интерфейс, обеспечивающий пользователю удобное взаимодействие с программой. Программа имеет связанные между собой модули: «UVIS v1.0 Сотрудник» — предназначен для оценщика, «UVIS v1.0 Кандидат» — для оцениваемого. «UVIS v1.0 Сотрудник» представляет собой форму, которая заполняется сотрудником, содержит в себе такие поля, как «Фамилия Имя Отчество кандидата», «Структурное подразделение», «Категория», а также анкету и идентификатор, присвоенный данной форме. «UVIS v1.0 Кандидат» содержит в себе идентификатор и тест, на который кандидат отвечает самостоятельно.

Автоматизация невозможна без наличия оборудованного рабочего места, которое включает в себя персональный компьютер, принтер и доступ в Интернет. Практика показывает, что многие организации используют две операционные системы: Windows XP и Windows 7. Разработчиком обеспечена работоспособность продукта на обеих операционных системах семейства Windows во всех существующих редакциях. В связи с тем, что доступ к персональному компьютеру необходим кандидату на вакантную должность, системному администратору необходимо произвести настройки дополнительной учетной записи таким образом, чтобы не допустить несанкционированного доступа к файлам и папкам.

Разработчик, как правило, дополняет свой продукт новыми функциями, изменяет внешний вид, исправляет ошибки предыдущей версии. Этот аспект актуален и для разработанной программы «UVIS v1.0». Реализация обновления возможна путем скачивания новой версии программы, при этом перед разработчиком стоит задача обеспечения сохранности базы данных и специфичных настроек, присущих данной организации, в которой используется продукт.

Для того чтобы программа могла быть адаптирована в любой организации, она

должна содержать в себе изменяемый блок вопросов, в котором отражена специфика сферы деятельности организации, отдельных структурных подразделений и должностей. Поставленная задача решена дополнительным модулем «UVIS v1.0. Конструктор», с помощью которого заказчик может сам составить вопросы, ответы на которые считает необходимыми для оценивания кандидата.

Важнейшим звеном в процессе оценки кандидата является сотрудник, который проводит оценку. Он должен быть ИТ-компетентным, способным легко освоить программный продукт. Проблемой является процесс обучения персонала, чей уровень владения персональным компьютером низок. В таком случае есть несколько вариантов решения данного вопроса. Первый — отказаться от автоматизированной версии, провести оценку, имея анкету-опросник на бумажном носителе, второй — обучить сотрудника минимальному набору знаний, достаточному для осуществления оценки по внедряемой методике.

Таким образом, созданный программный продукт позволяет автоматизировать процесс оценки кандидата на вакантную должность в контексте информационной безопасности. Со стороны пользователя данного продукта автоматизация процесса зависит от готовности как технической (наличие автоматизированного рабочего места и доступа в Интернет), так и кадровой (уровень владения персональным компьютером конечным пользователем). Нерешенными проблемами методики являются объективность оценщика и интерпретация нешаблонных ответов и фактов, касающихся оцениваемого. Открытым для разработчика остается вопрос процедуры обновления версии программы без потери базы данных и специфических настроек.

**Примечания**


[1] Азаров, А. А. Ускорение расчетов оценки защищенности пользователей информационной системы за счет элиминации маловероятных траекторий социоинженерных атак / А. А. Азаров, А. Л. Тулупьев, Н. Б. Соловцов, Т. В. Тулупьева // Труды СПИИРАН. — 2013. — Вып. 2 (25). — С. 171—181.

[2] Астахова, Л. В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации / Л. В. Астахова // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление и радиоэлектроника». — 2013. — Т. 13. — № 1. — С. 79—83.

[3] Астахова, Л. В. Методика оценки кадровых уязвимостей информационной безопасности организации на этапе приема сотрудника на работу / Л. В. Астахова, О. О. Землянская // Вестник УрФО. Безопасность в информационной сфере. — 2013. — № 1. — С. 53—59.

[4] Ванюшичева, О. Ю. Количественные измерения поведенческих проявлений уязвимостей пользователя, ассоциированных с социоинженерными атаками / О. Ю. Ванюшичева, Т. В. Тулупьева, А. Е. Пащенко, А. Л. Тулупьев, А. А. Азаров // Труды СПИИРАН. — 2011. — Вып. 4 (19). — С. 34—47.


**References**


[1] Azarov, A. A., Tulup'ev, A. L., Solovtsov, N. B., Tulup'eva, T. V. Uskorenie raschetov otsenki zashchishchennosti pol'zovatelei informatsionnoi sistemy za schet eliminatsii maloveroyatnykh traektorii sotsio-inzhenernykh atak [Acceleration factor in estimation of protection of users of information systems due to elimination of low-probability trajectory of social and engineering attacks]//Trudy SPIIRAN.— 2013. — No. 2 (25).— P. 171—181.

[2] Astakhova, L. V. Problema identifikatsii i otsenki kadrovykh uyazvimostei informatsionnoi bezopasnosti organizatsii [Problem of identification and assessment of personnel vulnerability of information security]// Vestnik YuUrGU. Seriya Komp'yuternye tekhnologii, upravlenie i radioelektronika. — 2013. — Volume 13, No.1. — P. 79—83.

[3] Astakhova, L. V., Zemlyanskaya, O. O. Metodika otsenki kadrovykh uyazvimostei informatsionnoi bezopasnosti organizatsii na etape priema sotrudnika na rabotu [Methodology assessment of personnel vulnerability of information security on the stage of employee's employment]/ L. V. Astakhova, O. O. Zemlyanskaya // Vestnik UrFO. Bezopasnost' v informatsionnoi sfere. — 2013. — No.1.— P. 53—59.

[4] Vanyushicheva, O. Yu., Tulup'eva, T. V. , Pashchenko, A. E., Tulup'ev, A. L., Azarov, A. A. Kolichestvennye izmereniya povedencheskikh proyavlenii uyazvimostei pol'zovatelya, assotsiirovannykh s sotsioinzhenernymi atakami [Quantitative evaluation of behavioristic activity in user's vulnerability associated with sociological and engineer attacks]//Trudy SPIIRAN. — 2011. — No. 4 (19). — P. 34—47.

**Астахова Людмила Викторовна,** д. п. н., профессор, профессор кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: lvastachova@mail.ru

**Землянская Ольга Олеговна,** студент кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: olka-balolka@rambler.ru

**Ефремов Виктор Александрович,** студент кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: efremovva@bk.ru

**Liudmila Viktorovna Astakhova,** PhD Pedagogics, professor, professor of the Department of Information System Security of the South Ural State University. E-mail: lvastachova@mail.ru

**Olga Olegovna Zemlianskaya,** student of the Department of Information System Security of the South Ural State University. E-mail: olka-balolka@rambler.ru

**Viktor Aleksandrovich Efremov,** student of the Department of Information System Security of the South Ural State University. E-mail: efremovva@bk.ru

УДК 004.056 + 002:004.056.5 + 005.922.1
ББК Х401.114

**Макарова П. В.**

# *ВВЕДЕНИЕ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ*

*В статье рассматриваются этапы введения режима коммерческой тайны, необходимые меры по охране конфиденциальности информации в соответствии с законодательством Российской Федерации: составление перечня сведений, составляющих коммерческую тайну; ограничение доступа к информации; учет лиц, получивших доступ к коммерческой тайне; регулирование отношений с работниками и контрагентами; нанесение грифа «Коммерческая тайна» на носители. Предложены рекомендации по указанным мерам и документационное сопровождение процесса введения режима коммерческой тайны. Рассмотрена ответственность за нарушение режима коммерческой тайны, приведены примеры из судебной практики.*

***Ключевые слова:*** *информация, составляющая коммерческую тайну; защита информации; режим коммерческой тайны; перечень информации, составляющей коммерческую тайну; разглашение.*

**Makarova P. V.**

# *THE INTRODUCTION OF COMMERCIAL SECRET REGIME*

*The article considers the stages of the introduction of commercial secret regime, as well as the following necessary measures of protection of information confidentiality in accordance with the Russian legislation: drawing up the list of information considered commercially secret; restriction of access to information; registration of individuals who have received access to commercial secrets; the regulation of relationships with employees and counterparties; application of the label "Commercial secret" on the media. The author suggests recommendations for mentioned measures and document support for the process of introduction of commercial secret regime. The author also deals with the responsibility for violation the above mentioned regime, and gives examples from judicial practice.*

***Keywords:*** *information constituting commercial secrets, information security, commercial secret regime, list of information constituting commercial secrets, disclosure.*

Вопросы защиты коммерческих секретов в условиях конкурентной борьбы очень актуальны. При этом собственники информации не уделяют должного внимания введению режима коммерческой тайны, пренебрегают требованиями законодательства, вследствие чего могут столкнуться с трудностями при защите своих интересов, что подтверждает и судебная практика.

В 2004 году был принят Федеральный закон «О коммерческой тайне», который закрепляет перечень мер по охране конфиденциальности в статье 10. Кроме того, в данном законе прописано, что режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, всех мер, указанных в законе[10]. Обратимся к мерам по охране конфиденциальности.

**1. Определение перечня информации, составляющей коммерческую тайну.** В законе указано, что право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит ее обладателю. Основываясь на определении информации, составляющей коммерческую тайну, данном в законе, можно сделать вывод, что критериями для отнесения информации к разряду ограниченного доступа являются:

- действительная или потенциальная коммерческая ценность;
- неизвестность третьим лицам;
- недоступность на законном основании[10].

Простая, на первый взгляд, задача может стать камнем преткновения при защите интересов в суде. Примером, подтверждающим это, служит Постановление апелляционного Тринадцатого арбитражного суда от 27.02.2007 г. по делу № А56-39537/2006, в котором основанием для удовлетворения требования о признании недействительным предписания антимонопольной службы о прекращении нарушения антимонопольного законодательства, выразившегося в использовании в предпринимательской деятельности информации, содержащей коммерческую тайну, служит то, что данная информация размещена на сайтах Интернета и является общедоступной[15].

Большое внимание должен уделить обладатель информации, составляющей коммерческую тайну, составлению Перечня информации, составляющей коммерческую тайну, учитывая ограничения. Во-первых, к коммерческой тайне не относится информация ограниченного доступа других видов: секретная (государственная тайна)[9] и конфиденциальная (персональные данные, профессиональная тайна, служебная тайна и др.)[13]. Кроме того, что отнесение других видов информации ограниченного доступа к коммерческой тайне противоречит законодательству, это является нецелесообразным, поскольку у каждого из этих видов информации свои цели защиты, определенный круг допущенных лиц, свои правила обработки такой информации. Во-вторых, запрещено относить к информации ограниченного доступа сведения, которые должны быть общедоступными по законодательству. Перечень этих сведений закреплен в следующих нормативно-правовых актах: Федеральном законе «О коммерческой тайне» (ст. 5)[10], Федеральном законе «О государственной тайне» (ст. 7)[9], Федеральном законе «Об информации, информационных технологиях и защите информации» (ст. 8, п.4)[12], Налоговом кодексе Российской Федерации (ст. 102)[7], «Положении о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использования атомной энергии»[14] и других. При нарушении перечисленных статей нормативных правовых актов обладателю информации не следует рассчитывать на защиту своих интересов в суде, он может быть даже привлечен к ответственности. Подтверждением этого служит Постановление Федерального арбитражного суда Приволжского округа от 12.04.2005 года по делу № А06-2626/1-6/04, в котором закреплено, что сведения, содержащиеся в учредительных документах обществ с ограниченной ответственностью, являются общедоступными, в отношении данных сведений не может быть установлен режим коммерческой тайны и они не подлежат защите гражданско-правовыми способами, следовательно, разглашение участником Общества третьим лицам сведений, содержащихся в учредительных документах Общества, о составе участников Общества, размере их долей и местожительстве, являющихся общедоступными в силу закона, не может повлечь ответственность участника Общества[17].

В литературе по защите коммерческой тайны можно встретить примерные перечни информации, составляющей коммерческую тайну[6]. Однако прибегать к таким перечням не рекомендуется, обладатель информации должен самостоятельно составить подобный перечень, поскольку это является уникальной задачей для каждой организации: то, что для одной организации будет информацией ограниченного доступа, другой может использоваться в рекламных целях.

Специалисты по конфиденциальному делопроизводству (Н. Н. Куняев, А. В. Некраха, Н. Г. Бутакова, В. А. Семенеко, А. И. Алексенцев) рекомендуют определить сроки ограничения доступа к информации[1, 2, 6, 8]. Действительно, без конкретных сроков конфиденциальности информация, составляющая коммерческую тайну, должна будет защищаться постоянно, в то время как ее коммерческая ценность может стремительно уменьшаться. Сроки могут ука-

зываться как определенные, так и в виде каких-либо событий, при наступлении которых информация станет общедоступной.

Кроме того, следует составить и перечень той информации, которая будет подлежать документированию. С введением такого перечня конкретизируется состав документов, на которые будет нанесен гриф ограничения доступа к документам. К разработке подобных Перечней рекомендуется привлекать специально созданную комиссию. Перечни подлежат утверждению должностным лицом либо документом[3, 11]. Кроме того, с Перечнями должны быть ознакомлены лица, допущенные к работе с информацией ограниченного доступа.

Очевидно, что при отсутствии Перечня не может быть речи о режиме коммерческой тайны и о защите интересов ее обладателя. Примером судебного решения может служить Постановление Федерального арбитражного суда Приволжского округа от 12.04.2005 года по делу № А06-2626/1-6/0, где иск о восстановлении на работу, взыскании заработной платы за время вынужденного прогула и компенсации морального вреда был правомерно удовлетворен, поскольку у работодателя отсутствовал перечень информации ограниченного доступа, в связи с чем увольнение работника за разглашение охраняемой законом тайны явилось незаконным[18].

**2. Ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.** Для того чтобы понять, как работает этот пункт статьи Федерального закона «О коммерческой тайне», обратимся к понятию «разглашение информации, составляющей коммерческую тайну». В законе оно определено как «действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору»[10]. «Бездействие» в данном случае можно трактовать как невыполнение определенных правил работы с информацией, составляющей коммерческую тайну, следовательно, необходимо эти правила регламентировать и требовать их выполнения.

Примером привлечения к ответственности за нарушение правил работы с информацией, составляющей коммерческую тайну, может быть отказ в удовлетворении исковых требований о признании увольнения работника незаконным, восстановлении на работе, взыскании заработной платы за время вынужденного прогула, поскольку увольнение работника за разглашение охраняемой законом коммерческой тайны было законным, так как работник допустил третье лицо к компьютеру с осуществленным входом в систему, а процедура и сроки наложения взыскания были соблюдены[19].

В делопроизводстве есть несколько видов документов методического характера. Это организационно-правовые документы, например, Положение о режиме коммерческой тайны, в котором может быть задокументирована все система защиты информации, составляющей коммерческую тайну, или же организационно-методические документы (инструкции, регламенты, правила, стандарты и др.), которые носят описательный характер работы с информацией ограниченного доступа. Например, рабочая инструкция по учету носителей конфиденциальной информации будет регламентировать лишь один процесс работы с информацией ограниченного доступа и будет предназначена для одного пользователя. Таким образом, обладатель информации может ввести один документ, регулирующий работу с коммерческой тайной, либо пакет дополняющих друг друга документов с условием, что они не будут дублировать друг друга. Последний вариант рекомендуется при разграничении доступа для выполнения различных процедур. В любом случае пользователи должны быть ознакомлены с инструктивными документами и проставить подписи за ознакомление. При этом следует учитывать, что чем детальнее будет прописан порядок работы с информацией ограниченного доступа, тем меньше вероятность ошибочных действий сотрудников, тем эффективнее будет осуществляться контроль соблюдения этого порядка. Контроль может проводиться в виде проверочных мероприятий с обязательной фиксацией результатов проверки.

**3. Учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана.** Законодатель не устанавливает конкретные

формы учета, что предоставляет свободу выбора обладателю информации. Учет может осуществляться в отдельной учетной форме (журнал учета, перечень лиц), либо учетными данными могут быть дополнены следующие документы: Перечень информации, составляющей коммерческую тайну; Перечень документов, содержащих информацию, составляющую коммерческую тайну; Номенклатура конфиденциальных дел. В любом случае должно быть получено согласие лица на ограничение своих прав (обязательство о неразглашении) проставлением его подписи.

**4. Регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.**

В соответствии с Трудовым кодексом РФ дополнительным условием трудового договора может являться условие о неразглашении охраняемой законом тайны (государственной, служебной, коммерческой и иной)[20].

В целях охраны конфиденциальности в рамках трудовых отношений работодатель обязан, в том числе, ознакомить работника под расписку с мерами ответственности за нарушение режима коммерческой тайны. Статья 14 Федерального закона «О коммерческой тайне» предусматривает дисциплинарную, гражданско-правовую, административную или уголовную ответственность за нарушение закона. Для работника, разгласившего информацию, составляющую коммерческую тайну, законодатель предусматривает дисциплинарную ответственность при отсутствии в его действиях состава преступления[10]. В статье 192 Трудового кодекса РФ за совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания: замечание, выговор, увольнение по соответствующим основаниям. Работодатель применяет дисциплинарное взыскание по своему усмотрению. При этом в статье 81 ТК РФ предусмотрена возможность расторгнуть трудовой договор по инициативе работодателя в случае неоднократного неисполнения работником без уважительных причин трудовых обязанностей, если он имеет дисциплинарное взыскание, или же однократного грубого нарушения работником трудовых обязанностей, коим, в том числе, является разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей[20].

При заключении договора с контрагентами необходимо также включить пункт о неразглашении информации, составляющей коммерческую тайну. При этом рекомендуется прописать срок конфиденциальности передаваемой информации, меру ответственности. Также в договоре с контрагентом можно зафиксировать конкретную сумму возмещения убытков при нарушении договорных обязательств по неразглашению информации, составляющей коммерческую тайну. В Гражданском кодексе Российской Федерации статья 1472 «Ответственность за нарушение исключительного права на секрет производства» обязывает нарушителя возместить убытки, причиненные нарушением исключительного права на секрет производства, если иная ответственность не предусмотрена законом или договором с этим лицом. В свою очередь статья 15 «Возмещение убытков» гласит, что лицо, право которого нарушено, может требовать полного возмещения причиненных ему убытков, если законом или договором не предусмотрено возмещение убытков в меньшем размере, что подразумевает и возмещение упущенной выгоды[4].

Уголовная ответственность за нарушение режима коммерческой тайны закреплена в Уголовном кодексе Российской Федерации, в котором предусмотрена статья 183 «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», которая предусматривает уголовную ответственность вплоть до лишения свободы до 7 лет[21].

К административной ответственности можно привлечь нарушителя в соответствии со статьей 1314 Кодекса об административных правонарушениях «Разглашение информации с ограниченным доступом»[5].

**5. Нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации.**

Следует отметить, что гриф должен быть нанесен на все носители информации, со-

ставляющей коммерческую тайну: бумажные, машинные, образцы изделий и другие (в отличие от защиты персональных данных, например, где нужно маркировать только машинные носители). Кроме того, до введения в действие Федерального закона «О коммерческой тайне» на практике применялись другие формулировки в грифе ограничения доступа: «Конфиденциально», «Строго конфиденциально», «КТ», «Для служебного пользования». Однако закон устранил разноголосицу в названиях, закрепив формулировку «Коммерческая тайна». Также в соответствии с законом с грифом указывается обладатель информации:

• для юридических лиц — полное наименование и местонахождение;

• для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства.

Так, Окружной суд Волго-Вятского округа посчитал правомерным вывод предыдущих судов о непринятии ОАО «Уралвагонзавод» всех необходимых мер для охраны конфиденциальной информации. Установлено, что нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации является одной из таких мер. Доказательств нанесения соответствующей информации на чертежи своей продукции истец не представил[16].

Наряду с указанными мерами обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры[10].

Перечисленные меры по охране конфиденциальности являются необходимыми и достаточными для введения режима коммерческой тайны на предприятии и гарантируют защиту интересов обладателя информации, составляющей коммерческую тайну, в суде. При этом судебная практика показывает, что если при введении режима коммерческой тайны хотя бы одна из 5 мер, указанных в законе, останется без внимания, это будет приравнено к тому, что режим коммерческой тайны не вводился вовсе, следовательно, нарушения режима останутся безнаказанными. Кроме того, стоимость внедрения мер по охране конфиденциальности, как правило, значительно ниже, чем действительная и потенциальная коммерческая ценность защищаемой информации. Таким образом, введение режима коммерческой тайны является эффективным способом защиты своих законных интересов и по силам каждой организации.

**Литература**


[1] Алексенцев, А. И. Конфиденциальное делопроизводство / А. И. Алексенцев. — М. : Управление персоналом, 2003. — 200 с.

[2] Бутакова, Н. Г. Защита и обработка конфиденциальных документов : учебн. пособие / Н. Г. Бутакова, В. А. Семенеко. — М. : МГИУ, 2008. — 284 с.

[3] Государственная система документационного обеспечения управления. Основные положения. Общие требования к документам и службам документационного обеспечения (одобрена коллегией Главархива СССР от 27.04.1988, Приказ Главархива СССР от 23.05.1988 № 33. — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=94185;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.9157000733539462. 3агл. с экрана.

[4] Гражданский кодекс Российской Федерации (Ч. 4) от 18.12.2006 № 230-ФЗ (ред. от 23.07.2003). — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=148685;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.38590494310483336. 3агл. с экрана.

[5] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2014). — http://base.consultant.ru/cons/cgi/online.cgi?req=doc; base=LAW;n=158526;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.7956647693645209. 3агл. с экрана.

[6] Куняев, Н. Н. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. — М. : Логос, 2011. — 452 с.

[7] Налоговый кодекс Российской Федерации (Ч. 1) от 31.07.1998 № 146-ФЗ (ред. от 28.12.2013). — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW; n=148796;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.5005321791395545. 3агл. с экрана.

[8] Некраха, А. В. Организация конфиденциального делопроизводства и защита информации : учеб. пособие / А. В. Некраха, Г. А. Шевцова. — М. : Академический Проект, 2007. — 224 с.

[9] О государственной тайне : Федеральный закон от 21.07.1993 № 5485-1 (ред. от 21.12.2013). — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156018;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.4454038303811103. Загл. с экрана.

[10] О коммерческой тайне : Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 11.07.2011). — http://base.consultant.ru/cons/cgi/online.cgi?req=card;page=splus;tab=0;ts=3EADEB628C493995E3F0737CD46F1506. Загл. с экрана.

[11] О принятии и введении в действие государственного стандарта Российской Федерации : постановление Росстандарта РФ от 03.03.2003 № 65-ст (вместе с «ГОСТ Р 6.30-2003. Государственный стандарт Российской Федерации. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов»). — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=44595;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.7047099198680371. Загл. с экрана.

[12] Об информации, информационных технологиях и защите информации : федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 28.12.2013). — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156802;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.15699254255741835. Загл. с экрана.

[13] Об утверждении Перечня конфиденциального характера : указ Президента РФ от 06.03.1997 № 188 (ред. от 23.09.2005). — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW; n=55795;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.22203667950816453. Загл. с экрана.

[14] Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использования атомной энергии : постановление Правительства РФ от 03.11.1994 № 1233 (ред. от 20.07.2012). — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=133084;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.3660610623192042. Загл. с экрана.

[15] Постановление апелляционного Тринадцатого арбитражного суда от 27.02.2007 г. по делу № А56-39537/2006. — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=RAPS013; n=16809;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.12686871271580458. Загл. с экрана.

[16] Постановление Арбитражного суда Волго-Вятского округа от 04.07.2008 г. по делу № А79-2693/2007. — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=AVV;n=28051;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.8914243641775101. Загл. с экрана.

[17] Постановление Федерального арбитражного суда Приволжского округа от 12.04.2005 года по делу № А06-2626/1-6/0. — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=APV; n=27366;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.6206985674798489. Загл. с экрана.

[18] Постановление Федерального арбитражного суда Приволжского округа от 12.04.2005 года по делу № А06-2626/1-6/0. — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ ;n=140753;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.42282360699027777. Загл. с экрана.

[19] Постановление Федерального арбитражного суда Приволжского округа от 12.04.2005 года по делу № А06-2626/1-6/0. — http://base.consultant.ru/cons/cgi/online.cgi?req=doc; base=SOJ;n=140753;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.0914941334631294. Загл. с экрана.

[20] Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. 28.12.2013). — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156601;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.3998664778191596. Загл. с экрана.

[21] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=158516;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.7333373171277344. Загл. с экрана.

## References


[1] Federal Law as of 29.07.2004 No.98-FZ (editorship as of 11.07.2011) «On commercial secrets» [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=card;page=splus;tab=0;ts=3EADEB628C493995E3F0737CD46F1506.

[2] Resolution of the Appeal 13th Arbitration Court as of 27.02.2007 on the case No. A56-39537/2006 [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=RAPS013; n=16809;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.12686871271580458.

[3] Federal Law as of 21.07.1993 No. 5485-1 (editorship as of 21.12.2013) «On state secrets» [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156018;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.4454038303811103.

[4] Russian Federation Presidential Decree as of 06.03. 1997 No. 188 (editorship as of 23.09.2005) «On the establishment of the list of confidential nature» [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW; n=55795;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.22203667950816453.

[5] Federal Law 27.07.2006 No. 149-FZ (editorship as of 28.12.2013) «On information, information technologies and information security» [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156802;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.15699254255741835.

[6] Taxation Code of the Russian Federation (Part 1) as of 31.07.1998 No. 146-FZ (editorship as of 28.12.2013) [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW; n=148796;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.5005321791395545.

[7] Governmental Decree of the Russian Federation as of 03.11.1994 No. 1233 (editorship as of 20.07.2012) «On the establishment of Provision on access to official information of restricted access in federal bodies of executive power and authorized bodies of the use of nuclear energy» [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=133084;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.3660610623192042.

[8] Resolution of the Federal Arbitration Court of Privolzhsky district as of12.04.2005 on the case No. A06-2626/1-6/0 [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=APV; n=27366;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.6206985674798489..

[9] Kunyaev, N.N. Konfidentsial'noe deloproizvodstvo i zashchishchennyi elektronnyi dokumentooborot: uchebnik [Confidential documentation management and protected electronic documentation management: Course book] – Moscow: Logos Publ., 2011. – 452 p.

[10] Nekrakha, A.V. Organizatsiya konfidentsial'nogo deloproizvodstva i zashchita informatsii: uchebnoe posobie [Organization of confidential document management and information security: Study guide]. – Moscow: Akademicheskii Proekt Publ., 2007. – 224 p.

[11] Butakova, N.G., Semeneko V.A. Zashchita i obrabotka konfidentsial'nykh dokumentov: Uchebnoe posobie [Security and processing of confidential documents: Study guide]. – Moscow: MGIU Publ., 2008. – 284 p.

[12] Aleksentsev, A.I., Konfidentsial'noe deloproizvodstvo [Confidential document management]. – Moscow: OOO «Zhurnal «Upravlenie personalom» Publ., 2003 – 200 p.

[13] State system of document support of management. Fundamental provisions. General requirements to the documents and authorities of document support (approved by the collegiate organ of the State Archive of the USSR as of 27.04.1988, Order of the State Archive of the USSR as of 23.05.1988 No. 33 [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=94185;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.9157000733539462.

[14] Resolution of the Federal Agency on Technical Regulating and Metrology of the Russian Federation as of 03.03.2003 No.65-st «On adoption and introduction into operation of the state standard of the Russian Federation » (together with the state standard R 6.30-2003. State Standard of the Russian Federation. Unified document systems. Unified system of organizational and directive documentation. Requirements to the document completion ») [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=44595;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.7047099198680371.

[15] Resolution of the Federal Arbitration Court of Privolzhsky district as of 12.04.2005 on the case No. A06-2626/1-6/0 [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ ;n=140753;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.42282360699027777.

[16] Resolution of the Federal Arbitration Court of Privolzhsky district as of 12.04.2005 on the case No. A06-2626/1-6/0 [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc; base=SOJ;n=140753;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.0914941334631294.

[17] Labour code of the Russina Federation as of 30.12.2001 No. 197-FZ (editorship as of 28.12.2013) [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156601;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.3998664778191596.

[18] Civil Code of the Russian Federation (Part 1) as of 18.12.2006 No. 230-FZ (as of 23.07.2003) [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=148685;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.38590494310483336.

[19] Criminal Code of the Russian Federation as of 13.06.1996 No. 63-FZ [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=158516;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.7333373171277344.

[20] Administrative Code of the Russian Federation as of 30.12.2001 No. 195-FZ (editorship 03.02.2014) [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc; base=LAW;n=158526;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.7956647693645209.

[21] Resolution of the Arbitration Court of Volgo-Vyatsky district as of 04.07.2008 on the case No. A79-2693/2007 [Electronic resource]. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=AVV;n=28051;dst=0;ts=3EADEB628C493995E3F0737CD46F1506;rnd=0.8914243641775101.

**Макарова Полина Викторовна,** кандидат педагогических наук, доцент кафедры «Безопасность информационных систем» ФГБОУ ВПО «Южно-Уральский государственный университет». E-mail: Bespalovapv@mail.ru

**Polina Viktorovna Makarova,** cand. Sc. Pedagogics, associated professor of the Department of Information System Security of South Ural State University. E-mail: Bespalovapv@mail.ru

УДК 005.992.1 + 004.056
ББК У9(2)240

**Астахова Л. В., Томилов А. А.**

# *КОМПЕТЕНЦИИ МЕНЕДЖЕРА В ОБЛАСТИ КАДРОВОЙ БЕЗОПАСНОСТИ В ФЕДЕРАЛЬНЫХ ГОСУДАРСТВЕННЫХ ОБРАЗОВАТЕЛЬНЫХ СТАНДАРТАХ ТРЕТЬЕГО ПОКОЛЕНИЯ*

*В статье выявлено противоречие между потребностью в специалистах — менеджерах по кадрам, которые должны иметь компетенции в области кадровой безопасности, и проблемами реализации потенциала вузов в развитии этих компетенций. Это показал анализ ФГОС ВПО для подготовки менеджеров и специалистов по управлению персоналом. Сделан вывод о необходимости возложить ответственность за этот процесс организационной защиты информации на выпускников образовательных направлений в области информационной безопасности, а для интеграции деятельности служб информационной безопасности и подразделений по управлению персоналом — усилить подготовку последних в данной области.*

***Ключевые слова:*** *кадровая безопасность, защита информации, менеджер, управление персоналом, стандарт.*

**Astakhova L. V., Tomilov A. A.**

# *MANASGER'S COMPETENCY IN THE FIELD OF PERSONNEL SECURITY IN FEDERAL STATE EDUCATIONAL STANDARDS OF 3D GENERATION*

*The article reveals the contradiction between the demand for specialists (personnel managers competent in the field of personnel security) and the problems of implementation of potential of higher educational institutions in terms of competency in the field of personnel*

*security. These results were revealed in the process of the analysis of Federal State Education Standards of Higher Professional Education for managers and specialists in the field of personnel management. The author makes a conclusion on the necessity of laying responsibility for organizational information security on graduate students of higher educational institutions in the field of information security. For the integration of activities of information security authorities and subdivisions of information security the author proposes to intensify the trainings in this field.*

***Keywords:*** *personnel security, information security, manager, personnel management, standards.*

Кадровая безопасность — это процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом. На сегодняшний день специалисты, отвечающие за безопасность предприятий, организаций и учреждений, признают, что кадровая безопасность — это непременная и основная составная часть любой системы, которую организация формирует для защиты информации[2].

В современном обществе существует потребность в высококвалифицированных и профессионально подготовленных кадрах. При подготовке специалистов в той или иной сфере деятельности предъявляются требования ФГОС (федерального государственного образовательного стандарта) к результатам высшего профессионального образования, в настоящее время это ФГОС-3. Данные требования включают в себя следующие характеристики, необходимые выпускнику вуза: способность адаптироваться к постоянно меняющимся современным требованиям технического прогресса, ориентация на компетентное решение профессиональных задач, готовность к самосовершенствованию, самообразованию, самоконтролю, позволяющая реализовать свои потенциальные возможности, по-другому их можно назвать профессиональными компетенциями (ПК).

Важнейшими профессиональными компетенциями менеджера являются компетенции в области кадровой безопасности. Опираясь на мнение ученых, изучающих проблемы кадровой безопасности[1, 7], приведем необходимые составляющие деятельности современного менеджера:

• работа с анкетными данными, их проверка, составление;

• умение оценивать профессиональные компетенции, декларированные кандидатом;

• умение анализировать возможные угрозы от деятельности персонала, проводить мониторинг внутренних угроз;

• навык разработки документационного обеспечения кадровой безопасности;

• изучение лояльности и благонадежности персонала;

• разработка технологии увольнения для конкретных должностей;

• умение просчитывать риски, связанные с увольнением персонала;

• мониторинг факторов риска у персонала;

• оценка профессиональной мотивации сотрудников;

• развитие навыков, позволяющих взаимодействовать с людьми на уровне психологии;

• умение составлять полный психологический портрет конкретного лица;

• разработка процедур кадровой безопасности на период адаптации новых сотрудников;

• социально-психологическое исследование трудового коллектива на предмет совместимости сотрудников и комплектования наиболее эффективных групп для решения стоящих задач;

• разработка профессиональной аттестации персонала, направленной на нейтрализацию рисков, связанных с профессиональной некомпетентностью сотрудников.

Для того чтобы определить потенциальные возможности современного вуза подготовить менеджеров к названным видам работы, проанализируем Федеральные государственные образовательные стандарты по следующим образовательным направлениям: «Менеджмент» (бакалавриат)[3], «Управление персоналом» (бакалавриат)[4], «Менеджмент» (магистратура)[5], «Управление персоналом» (магистратура)[6].

ФГОС-3 по направлению (080200) «Менеджмент» (бакалавриат) включает следую-

щие компетенции, связанные с работой с кадрами:

Организационно-управленческая деятельность:

• способность эффективно организовать групповую работу на основе знания процессов групповой динамики и принципов формирования команды (ПК-5);

• способность участвовать в разработке стратегии управления человеческими ресурсами организаций, планировать и осуществлять мероприятия, направленные на ее реализацию (ПК-13).

Информационно-аналитическая деятельность:

• умение проводить аудит человеческих ресурсов и осуществлять диагностику организационной культуры (ПК-37).

ФГОС-3 по направлению (080400) «Управление персоналом» (бакалавриат) включает следующие компетенции, связанные с работой с кадрами:

Организационно-управленческая и экономическая деятельность:

• знание основ разработки и внедрения требований к должностям, критериев подбора и расстановки персонала и умение применять их на практике (ПК-5);

• знание основ найма, разработки и внедрения программ и процедур подбора и отбора персонала и умение применять их на практике (ПК-6);

• владение методами деловой оценки персонала при найме и готовность применять их на практике (ПК-7);

• знание основ профориентации персонала и умение применять их на практике (ПК-8);

• знание принципов формирования системы адаптации персонала, разработки и внедрения программ адаптации и умение применять их на практике (ПК-9);

• знание видов, форм и методов обучения персонала (ПК-12);

• знание основ управления карьерой и служебно-профессиональным продвижением персонала и умение применять их на практике (ПК-13);

• знание процедуры приема, увольнения, перевода на другую работу и перемещения персонала в соответствии с Трудовым кодексом Российской Федерации, владение навыками оформления сопровождающей документации (ПК-23);

• знание Гражданского кодекса Российской Федерации в части, относящейся к деятельности кадровой службы (ПК-26).

Информационно-аналитическая деятельность:

• знание основ проведения аудита и контроллинга персонала и умение применять их на практике (ПК-60).

ФГОС-3 по направлению (080200) «Менеджмент» (магистратура) включает следующие компетенции, связанные с работой с кадрами:

Организационно-управленческая деятельность:

• способность управлять организациями, подразделениями, группами (командами) сотрудников, проектами и сетями (ПК-1).

ФГОС-3 по направлению (080400) «Управление персоналом» (магистратура) включает следующие компетенции, связанные с работой с кадрами:

Организационно-управленческая и экономическая деятельность:

• умение разрабатывать и внедрять политику привлечения, подбора и отбора конкурентоспособного персонала (ПК-7);

• умение разрабатывать и внедрять политику адаптации персонала организации (ПК-8);

• умение разрабатывать и внедрять политику обучения и развития персонала организации (ПК-9).

Однако все ли из этих знаний, умений, навыков в области кадровой безопасности учтены при формулировке компетенций в ФГОС-3? Определим, в рамках каких компетенций могут формироваться названные составляющие деятельности специалиста в области кадровой безопасности:

Работа с анкетными данными, их проверка, составление (Знание основ проведения аудита и контроллинга персонала и умение применять их на практике (ПК-60)).

Умение оценивать профессиональные компетенции, декларированные кандидатом (Знание основ разработки и внедрения требований к должностям, критериев подбора и расстановки персонала и умение применять их на практике (ПК-5)).

Умение анализировать возможные угрозы от деятельности персонала, проводить мониторинг внутренних угроз (Умение проводить аудит человеческих ресурсов и осуществлять диагностику организационной культуры (ПК-37)).

Навык разработки документационного обеспечения кадровой безопасности (Знание

процедуры приема, увольнения, перевода на другую работу и перемещения персонала в соответствии с Трудовым кодексом Российской Федерации, владение навыками оформления сопровождающей документации (ПК-23)).

Разработка процедур кадровой безопасности на период адаптации новых сотрудников (Знание принципов формирования системы адаптации персонала, разработки и внедрения программ адаптации и умение применять их на практике (ПК-9)).

Социально-психологическое исследование трудового коллектива на предмет совместимости сотрудников и комплектования наиболее эффективных групп для решения стоящих задач (Способность эффективно организовать групповую работу на основе знания процессов групповой динамики и принципов формирования команды (ПК-5)).

Разработка профессиональной аттестации персонала, направленной на нейтрализацию рисков, связанных с профессиональной некомпетентностью сотрудников (Знание видов, форм и методов обучения персонала (ПК- 12)).

Определив соотношения, мы выявили некоторые из знаний и навыков, которые ни к одной из компетенций отнести невозможно:

- изучение лояльности и благонадежности персонала;
- разработка технологии увольнения для конкретных должностей;
- умение просчитывать риски, связанные с увольнением персонала;
- мониторинг факторов риска у персонала;
- оценка профессиональной мотивации сотрудников;
- развитие навыков, позволяющих взаимодействовать с людьми на уровне психологии;
- умение составлять полный психологический портрет конкретного лица.

Таким образом, можно сделать вывод, что многие ключевые составляющие деятельности современного специалиста по работе с персоналом и обеспечению кадровой безопасности, перечисленные выше, не предусмотрены ФГОС-3 по образовательным направлениям «Менеджмент» (бакалавриат), «Управление персоналом» (бакалавриат), «Менеджмент» (магистратура), «Управление персоналом» (магистратура). Возникает противоречие между потребностью в специалистах, которые должны иметь компетенции в области кадровой безопасности, и проблемами реализации потенциала вузов в развитии этих компетенций. При таком положении дел современные выпускники — специалисты по управлению персоналом или менеджеры — не обладают компетенциями для обеспечения кадровой безопасности организации, хотя зачастую на них возлагается эта работа. Поэтому ответственность за этот процесс организационной защиты информации может быть возложена только на выпускников образовательных направлений в области информационной безопасности. Для интеграции деятельности служб информационной безопасности и подразделений по управлению персоналом необходимо усилить подготовку последних в данной области, для чего следует внести дополнения не только в образовательные стандарты, но и в учебные планы и учебные программы, формы и методы обучения.

**Примечания**

[1] Астахова, Л. В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации / Л. В. Астахова // Вестник Южно-Уральского государственного университета. Серия «Компьютерные технологии, управление, радиоэлектроника». — 2013. — Т. 13. — № 1. — С. 79—83.

[2] Потапова, Л. А. Основы кадровой безопасности / Л. А. Потапова // Справочник кадровика. — 2005. — № 12. — С. 24—25.

[3] Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 080200 Менеджмент (квалификация (степень) «Бакалавр»). — http://fgosvo.ru/uploadfiles/fgos/8/20111115140436.pdf.

[4] Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 080400 Управление персоналом (квалификация (степень) «Бакалавр»). — http://fgosvo.ru/uploadfiles/fgos/8/20111115140457.pdf.

[5] Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 080200 Менеджмент (квалификация (степень) «Магистр»). — http://fgosvo.ru/uploadfiles/fgos/36/20110326211205.pdf.

[6] Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 080400 Управление персоналом (квалификация (степень) «Магистр»). — http://fgosvo.ru/uploadfiles/fgos/36/20110412233031.pdf.

[7] Чумарин, И. Г. Что такое кадровая безопасность компании / И. Г. Чумарин // Кадры предприятия. — 2003. — № 2. — http://www.bre.ru/security/20813.html.

**References:**


[1] Potapova, L. A. Osnovy kadrovoi bezopasnosti [Fundamentals of personnel security]/ L.A. Potapova // Spravochnik kadrovika. — 2005. — No. 12. — P. 24—25.

[2] Federal State Educational Standard of Higher Professional Education for the major No. 080200 Bachelor of Management [Electronic resource]. - http://fgosvo.ru/uploadfiles/fgos/8/20111115140436.pdf

[3] Federal State Educational Standard of Higher Professional Education for the major No. 080400 Bachelor of Personnel Management [Electronic resource]. — http://fgosvo.ru/uploadfiles/fgos/8/20111115140457.pdf

[4] Federal State Educational Standard of Higher Professional Education for the major No. 080200 Master of Management [Electronic resource]. - http://fgosvo.ru/uploadfiles/fgos/36/20110326211205.pdf

[5] Federal State Educational Standard of Higher Professional Education for the major No. 080400 Master of Personnel Management [Electronic resource]. — http://fgosvo.ru/uploadfiles/fgos/36/20110412233031.pdf

[6] Chumarin, I.G. Chto takoe kadrovaya bezopasnost' kompanii [What is a personnel security in a company?]/ I.G. Chumarin // Kadry predpriyatiya. — 2003. — No. 2 [Electronic resource]. - http://www.bre.ru/security/20813.html

[7] Astakhova, L. V. Problema identifikatsii i otsenki kadrovykh uyazvimostei informatsionnoi bezopasnosti organizatsii [Problem of identification and evaluation of personnel vulnerability of information security in a company]/ Astakhova L.V.// Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Komp'yuternye tekhnologii, upravlenie, radioelektronika. — 2013. V. 13. — No. 1. — P. 79—83.


---


**Астахова Людмила Викторовна,** д. п. н., профессор, профессор кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: lvastachova@mail.ru

**Томилов Александр Александрович,** аспирант кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: tomilov62@yandex.ru

**Liudmila Viktorovna Astakhova,** PhD Pedagogics, professor, professor of the Department of Information System Security of the South Ural State University. E-mail: lvastachova@mail.ru

**Aleksand Aleksandrovich Tomilov,** PhD student of the Department of Information System Security of the South Ural State University. E-mail: tomilov62@yandex.ru

УДК 004.056 + 005.96:004.056
ББК Х404.3(2)

**Астахова Л. В., Иванов Е. С.**

# *ТРЕБОВАНИЯ НОРМАТИВНЫХ АКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ К ИННОВАЦИОННОЙ КУЛЬТУРЕ СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ*

*Инновационное развитие как приоритетное направление деятельности Российской Федерации требует формирования необходимых навыков, компетенций и знаний каждого гражданина, в том числе и будущих специалистов по защите информации. В статье проведен анализ нормативных актов России по вопросам инновационной деятельности, в т. ч. «Стратегии инновационного развития Российской Федерации на период до 2020 года», в которой отдельный раздел посвящен инновационной культуре. При этом выявлена поверхностность в определении способов ее формирования, а также недостатки ФГОС ВПО по информационной безопасности, который не отражает актуальных требований к инновационной культуре будущего выпускника этого образовательного направления. Обоснована амбивалентность как специфическая особенность инновационной культуры специалиста по защите информации, который является одновременно субъектом и объектом инновационной культуры в организации, обнаружена ее обусловленность необходимостью обеспечения кадровой безопасности.*

***Ключевые слова:*** *инновационная культура, специалист, защита информации, нормативные акты, кадровая безопасность.*

**Astakhova L. V., Ivanov E. S.**

# *REQUIREMENTS OF STATUTORY ACTS OF THE RUSSIAN FEDERATION FOR INNOVATION CULTURE OF THE INFORMATION SECURITY SPECIALISTS*

*Innovation-driven development as a priority activity of the Russian Federation requires the formation of the necessary skills, competencies and knowledge of every citizen, including the*

*future information security specialists. The article analyzes Russian statutory acts and regulations on innovation, including "Innovation Development Strategy of the Russian Federation for the period of up to 2020" where a separate section is devoted to innovation culture. At the same time the article reveals the superficiality in determining the methods of its formation, as well as disadvantages of Federal State Education Standards of Higher Professional Education in information security which do not reflect the actual requirements for the innovation culture of the future graduates of this educational area. The author justifies the ambivalence as a specific feature of the innovation culture of information security specialists, which is both subject and object of the innovation culture in the organization in terms of ensuring personnel security.*

***Keywords:*** *innovation culture, specialists, information security, regulations, personnel security.*

Стремительный темп развития новых информационных технологий требует от специалистов по защите информации разработки и внедрения этих технологий в практику, а значит — высокого уровня инновационной культуры. Данный императив соответствует требованиям нормативных актов России. Область инноваций, инновационной деятельности и инновационного развития регулируется в Российской Федерации рядом нормативно-правовых актов. Основное определение инновации и инновационной деятельности закреплено в Федеральном законе № 127-ФЗ[1], который посвящен регуляции отношений между органами государственной власти, субъектами научной, научно-технической и инновационной деятельности, а также потребителями результатов такой деятельности. В рамках закона закреплены определения инновации, инновационного проекта, инновационной инфраструктуры и инновационной деятельности. Так, под инновационной деятельностью понимается «деятельность (включая научную, технологическую, организационную, финансовую и коммерческую деятельность), направленная на реализацию инновационных проектов, а также на создание инновационной инфраструктуры и обеспечение ее деятельности».

Инновациям посвящены также разделы и части в ряде других правовых актов: закона «Об образовании»[8], закона «О развитии предпринимательства»[2], закона «О техническом регулировании»[5], закона «О Сколково»[7] и ряде других.

В 1999 году был разработан проект закона[6], связанного исключительно с инновациями, однако он был отклонён Президентом РФ в 2000 году[9], пересмотрен специальной комиссией[4] в течение года и в 2001 году окончательно снят с рассмотрения. Отклонение проекта Президентом РФ было связано с рядом серьёзных замечаний: определение «инновационная деятельность» не позволяло чётко понять критерии отнесения деятельности к инновационной, а статья 3, раскрывающая содержание такой деятельности, противоречила предложенному определению.

Особое место в рамках системы актов об инновациях, инновационной деятельности и инновационной культуре занимает «Стратегия инновационного развития Российской Федерации на период до 2020 года»[11] (далее — Стратегия), утверждённая распоряжением Правительства РФ. Основная цель реализации документа — перевод экономики России к 2020 году на инновационный путь развития, характеризующийся рядом показателей: доля промышленных предприятий, осуществляющих инновации, доля экспорта высокотехнологичных продуктов, доля России на мировых рынках, количество патентов на душу населения, количество цитирований российских работ в научных журналах и другие.

Стратегия нацелена на решение основных задач инновационного развития Российской Федерации: развитие кадрового потенциала в науке и образовании, повышение инновационной активности бизнеса, реализация инновационной политики органами государственной власти, создание материальных и моральных стимулов для притока специалистов, повышение восприимчивости населения к инновациям и другие.

Инновационная политика занимает особое положение в системе социально-экономической деятельности государства. Так, её элементы включены в:

- бюджетную политику — в части обеспечения приоритетности инновационных расходов и определения параметров основных статей расходов бюджета, необходимых для развития инноваций;
- налоговую политику — в части оптимизации уровня налоговой нагрузки на базовые факторы инновационного развития, а также в части введения необходимых налоговых льгот;
- техническую политику — в части формирования системой технического регулирования стимулов к технологической модерни-

зации и инновациям, а также к снятию барьеров и ограничений на внедрение новых технологий;

• конкурентную политику и политику в сфере борьбы с коррупцией — в части минимизации возможностей для несправедливой конкуренции через использование административного ресурса, в части предотвращения и пресечения антиконкурентных действий доминирующих на рынках хозяйствующих субъектов, а также в части формирования благоприятного предпринимательского климата, включая деятельность правоохранительных и контрольных органов, судебной системы, конкурентоспособность российской юрисдикции, общее правовое регулирование создания и ведения бизнеса;

• политику в сфере государственных закупок — в части создания необходимых инструментов и процедур, дающих возможность государственным заказчикам закупать инновационную продукцию, а государству в целом — стимулировать за счёт государственных закупок создание такой инновационной продукции;

• внешнюю и внешнеэкономическую политику — в части более активного отстаивания интересов российских инновационных компаний на внешних рынках, а также в части поиска за рубежом технологических партнёров для российских предприятий, способных оказать значимое содействие в технологической модернизации российской экономики;

• региональную политику — в части установления более высокого приоритета поддержки тех регионов, которые инвестируют в инновационное развитие.

В Стратегии характеризуются современное состояние и проблемы инновационного развития РФ, в том числе определяются вызовы инновационного развития. Документ подчёркивает, что акты, посвящённые проблемам развития инноваций и инновационной деятельности: «Стратегия развития науки»[13] и «Политика РФ в области развития инновационной системы»[12], — принятые ранее, требовали пересмотра в связи с мировым экономическим кризисом 2008—2009 годов. В Стратегии отмечается важность достижения установленных ранее показателей инновационной активности, то есть не пересмотра их в сторону уменьшения, а разработки новых рекомендаций и мер для интенсивного роста.

Среди проблем инновационного развития отмечаются следующие: низкий спрос на результаты интеллектуальной деятельности, преимущественно бюджетное формирование объёма средств, низкая отдача от технологических инноваций, низкий уровень восприимчивости инноваций бизнес-структурами (9,4 %, по сравнению с Германией — 71,8 %, Бельгией — 53,6 %, Эстонией — 52,8 %) и недостаточность развития личностных качеств — мобильности, желания постоянно обучаться. Так, доля участия населения в непрерывном образовании в 2008 году по данным Федеральной службы государственной статистики составила 24,8 %, тогда как показатели наиболее активных европейских стран в инновационной сфере следующие: Финляндия — 77,3 %, Германия — 41,9 %, Великобритания — 37,6 %.

Проблемой инновационного развития является и скромное положение российских компаний на мировых рынках высокотехнологичной продукции. В 2008 году доля экспорта продукции составила 0,25 %, в то время как лидирующие страны — Китай, США и Германия — имеют соответственно 16,3 %, 13,5 % и 7,6 %.

Трудности для реализации Стратегии создаёт также недостаточное финансирование сферы образования и науки. В 2009 году Российская Федерация тратила на образование 4,6 % ВВП. Для сравнения, США — 5 %, Великобритания — 5,2 %, Франция — 5,5 %, Швеция — 6,1 %.

Ключевой проблемой инновационного развития России остаётся низкая отдача от технологических инноваций. Если в абсолютном значении подобные показатели растут, так, с 1995 года по 2009 год отмечается рост объёмов на 34 %, то в удельном соотношении с затратами наблюдается совершенно иная картина — на 1 рубль затрат на инновации в 1995 году приходилось 5,5 рубля инновационной продукции, а в 2009 году — 2,4 рубля.

В документе рассматриваются три основных пути инновационного развития: инерционный, вариант догоняющего развития и вариант достижения лидерства. Под инерционным способом развития понимается такой путь, при котором инновации импортируются у стран-лидеров, а государство лишь развивает вспомогательную инфраструктуру. Затраты при таком подходе минимальны, но существует серьёзный риск роста отставания от инновационно-развитых стран. Ярким примером использования догоняющего варианта развития является Китай. При таком способе приоритет отдаётся внутренним разработкам, а при их отсутствии технологии (причём не самые передовые) импортируются, а затем дорабатываются под конкретные нужды. И, наконец, вариант достижения лидерства. При таком пути развития ставятся задачи не только использования внутренних разработок, но и вывода их на мировой рынок и достижения позиций лидера в экспорте инноваций. Подобный путь полностью отве-

чает требованиям и целям стратегии развития России. Однако в силу существенных затрат он не может быть сразу применён. Поэтому наиболее оптимальным для России является сочетание лидирующего положения в приоритетных отраслях — оборонной, ядерной промышленности, авиастроении и так далее — и догоняющего пути развития в отстающих отраслях, с их последующим развитием до лидирующих позиций.

Разработчики Стратегии предлагают инновационное развитие России провести в два этапа. На первом решается задача повышения восприимчивости бизнеса и экономики к инновациям, формируются основы для создания инфраструктуры. На втором этапе повышается доля расходов на науку и инновации, происходит окончательное формирование инновационной инфраструктуры, достигаются лидирующие показатели по отдельным отраслям.

Одним из направлений реализации Стратегии определена необходимость создания технопарков и технологических центров для формирования благоприятной среды коллективного использования научного оборудования. Подобная необходимость обусловлена крайне высокими затратами на приобретение необходимых приборов и устройств, зачастую такие издержки становятся серьёзным барьером для малых инновационных предприятий. Использование научного оборудования на правах аренды в рамках технопарков позволит сделать инновации доступными для широкого круга предприятий различных форм собственности. На момент утверждения Стратегии в России действовало более 140 инновационно-технологических центров и технопарков, запланировано до конца 2014 года выделение средств ещё на 12 подобных объектов.

Технопарки являются неотъемлемой частью инновационной инфраструктуры наряду с инновационными бизнес-инкубаторами, национальными исследовательскими университетами и созданными на базе высших учебных заведений малыми предприятиями для коммерциализации новых перспективных разработок. Яркий пример подобного объекта — инновационный центр «Сколково». В соответствии с Федеральным законом «Сколково» — совокупность инфраструктуры территории инновационного центра и механизмов взаимодействия лиц, участвующих в реализации проекта, в том числе путём использования этой инфраструктуры. Так, в состав центра входят собственный технопарк, пять инновационных кластеров: кластер биомедицинских технологий, кластер информационных и компьютерных технологий, кластер космических технологий и телекоммуникаций, кластер энергоэффективных технологий, кластер ядерных технологий — а также образовательные проекты — открытый университет Сколково и Сколковский институт науки и технологий. К тому же «Сколково» — особая экономическая зона, в рамках которой действуют налоговые льготы, упрощены механизмы лицензирования и государственной регистрации. Эти условия создают благоприятную обстановку для привлечения международных инвестиций. Так, в рамках центра открыты (или планируются к открытию в ближайшее время) площадки таких компаний, как Nokia, Siemens, Microsoft, Intel, Cisco и другие. По заявлению исполнительного директора кластера ядерных технологий Игоря Караваева, в октябре 2013 года «Сколково» насчитывало более 1000 участников[14].

Одной из основных задач инновационного развития является создание условий для формирования у граждан следующих компетенций инновационной деятельности[11]:

• способности и готовности к непрерывному образованию, постоянному совершенствованию, переобучению и самообучению, профессиональной мобильности, стремления к новому;

• способности к критическому мышлению;

• способности и готовности к разумному риску, креативности и предприимчивости, умения работать самостоятельно, готовности к работе в команде и в высококонкурентной среде;

• владения иностранными языками, предполагающего способность к свободному бытовому, деловому и профессиональному общению.

Отдельная часть Стратегии посвящена развитию культуры инноваций. Отмечается, что создание необходимых культурных предпосылок, а также проведение активной информационной и образовательной политики являются важными условиями активизации инновационной деятельности. Среди предложенных мер встречаются: создание кинофильмов и телесериалов, популяризующих научную и изобретательскую деятельности, а также создание специализированных средств массовой информации о науке и инновациях. Развитие культуры инноваций предполагается проводить с помощью информационного воздействия, направленного на повышение престижа науки и образования и содействие широкому публичному обсуждению проблем, касающихся научных исследований и инноваций в Российской Федерации. Для закрепления результатов предлагается учредить премию, например, «За лучший инновационный продукт».

Государство в ходе реализации Стратегии призвано выполнять координационные функции. Так, общее руководство до августа 2012 года осуществляла Правительственная комиссия по высоким технологиям и инновациям. После её упразднения[10] функции координатора Стратегии перешли к Совету по модернизации экономики и инновационному развитию России[3]. Отдельные министерства и ведомства также задействованы в регуляции инновационной деятельности. На Министерство экономического развития Российской Федерации, например, возложены полномочия по координации действий федеральных органов исполнительной власти в сфере стимулирования спроса на инновации со стороны реального сектора экономики, а на Министерство образования и науки Российской Федерации — по координации работы по формированию предложений для развития инновационной экономики со стороны сектора исследований и разработок.

Результаты анализа деятельности государства в сфере инноваций за последние 5 лет позволяют сделать ряд выводов. Несмотря на негативные факторы влияния, названные в начале, отмечается рост доли участия населения в непрерывном образовании на 2,5 % до уровня 27,3 % к 2012 году. В 2010 году этот показатель составлял 30,4 %. Снижение показателя связано, скорее всего, с последствиями того же экономического кризиса 2009 года — в связи с ухудшением экономических показателей практически все компании перешли к стратегии снижения издержек, и среди затрат, которые были сокращены при этом, чаще всего уменьшались расходы на обучение сотрудников.

Россия обладает хорошим человеческим капиталом для достижения целей Стратегии. Наряду с уровнем непрерывного образования наше государство является одним из лидеров по уровню образованности населения. В России 22,8 % населения имеют высшее или дополнительное профессиональное образование. Этот показатель сопоставим с долей образованного населения в таких странах, как Великобритания, Япония, Германия.

Стратегия инновационного развития Российской Федерации является основополагающим документом в области науки, инноваций и инновационной деятельности. Любая деятельность, связанная с новыми технологиями, в том числе и формирование инновационной культуры будущих специалистов по защите информации, должна основываться на положениях Стратегии. Полагаем, что следует сформулировать следующие требования к инновационной культуре специалистов по защите информации, основываясь на требованиях, названных в Стратегии: наличие способности к критическому мышлению; наличие способности и стремления к непрерывному образованию; стремление к новому; профессиональная мобильность; креативность; предприимчивость; умение работать как самостоятельно, так и в команде; знание иностранных языков на уровне уверенного разговорного.

Необходимость развития названных компетенций специалистов по защите информации, к сожалению, не нашла отражения в федеральном государственном образовательном стандарте высшего профессионального образования по направлению подготовки «Информационная безопасность». Некоторые компетенции, которые должны быть сформированы у специалистов по защите информации согласно ФГОС, косвенно связаны с предложенным перечнем, но прямого указания на необходимость формирования инновационной культуры в стандарте нет.

Таким образом, инновационное развитие — приоритетное направление деятельности Российской Федерации, и формирование необходимых навыков, компетенций и знаний — задача каждого гражданина, в том числе и будущих специалистов по защите информации. Россия лишь начинает своё движение по пути инноваций, лишь формирует основы для успешного ведения инновационной деятельности, лишь задаёт курс дальнейшего социально-экономического роста. Анализ нормативных актов России по вопросам инновационной деятельности показал, что особое место среди них принадлежит «Стратегии инновационного развития Российской Федерации на период до 2020 года», в которой детально рассмотрены критерии, связанные с экономическими аспектами и проблемами развития инновационной инфраструктуры. Отдельный раздел документа посвящен инновационной культуре, однако требования к ней описаны поверхностно, без глубокого раскрытия и определения способов достижения цели. Специфической особенностью инновационной культуры специалиста по защите информации является её двойственность: с одной стороны, он должен сам быть с инновациями на «ты», с другой — должен быть примером для других сотрудников организации. Эта особенность связана с таким направлением деятельности защитников информации, как кадровая безопасность, которая, в свою очередь, направлена на обучение персонала, его развитие и т. д. ФГОС ВПО по информационной безопасности не отражает актуальных требований к инновационной культуре выпускников, что ставит перед педагогической наукой задачу поиска решения данной проблемы.

## Примечания

[1] О науке и государственной научно-технической политике : Федеральный закон РФ от 23 августа 1996 г. № 127-ФЗ // Собрание законодательства РФ. — 1996. — № 35. — Ст. 4137.

[2] О развитии малого и среднего предпринимательства в Российской Федерации : Федеральный закон от 24 июля 2007 г. № 209-ФЗ // Собрание законодательства РФ. — 2007. — № 31. — Ст. 4006.

[3] О Совете при Президенте Российской Федерации по модернизации экономики и инновационному развитию России : Указ Президента РФ от 18 июня 2012 г. № 878 // Собрание законодательства РФ. — 2012. — № 26. — Ст. 3499.

[4] О создании специальной комиссии в связи с отклонением Президентом Российской Федерации Федерального закона «Об инновационной деятельности и о государственной инновационной политике» : Постановление ГД ФС РФ от 18 февраля 2000 г. № 93-III ГД // Собрание законодательства РФ. — 2000. — № 9. — Ст. 1007.

[5] О техническом регулировании : Федеральный закон от 27 декабря 2002 г. № 184-ФЗ // Собрание законодательства РФ. — 2002. — № 52 (Ч. 1). — Ст. 5140.

[6] О Федеральном законе «Об инновационной деятельности и о государственной инновационной политике» : постановление ГД ФС РФ от 21 июня 2001 г. № 1664-III ГД (проект № 99029071-2) // Собрание законодательства РФ. — 2001. — № 27. — Ст. 2710.

[7] Об инновационном центре «Сколково» : Федеральный закон от 28 сентября 2010 г. № 244-ФЗ // Собрание законодательства РФ. — 2010. — № 40. — Ст. 4970.

[8] Об образовании в Российской Федерации : Федеральный закон РФ от 29 декабря 2012 г. № 273-ФЗ // Собрание законодательства РФ. — 2012. — № 53 (Ч. 1). — Ст. 7598.

[9] Об отклонении принятого Государственной Думой 1 декабря 1999 г. Федерального закона «Об инновационной деятельности и о государственной инновационной политике» : Письмо Президента РФ от 3 января 2000 г. № Пр-14 // Справочно-правовая система «КонсультантПлюс». — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=4195.

[10] Об упразднении Правительственной комиссии по высоким технологиям и инновациям : постановление Правительства РФ от 16 августа 2012 г. № 839 // Собрание законодательства РФ. — 2012. — № 35. — Ст. 4828.

[11] Об утверждении Стратегии инновационного развития Российской Федерации на период до 2020 года : Распоряжение Правительства Российской Федерации от 8 декабря 2011 г. № 2227-р // Собрание законодательства РФ. — 2012. — № 1. — Ст. 216.

[12] Основные направления политики Российской Федерации в области развития инновационной системы на период до 2010 года : Постановление Правительства РФ от 05 августа 2005 г. № 2473п-П7 // Справочно-правовая система «КонсультантПлюс». — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=91912.

[13] Стратегия развития науки и инноваций в Российской Федерации на период до 2015 года : протокол Межведомственной комиссии по научно-инновационной политике от 15 февраля 2006 г. № 1 // Справочно-правовая система «КонсультантПлюс». — http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=101907;fld=134;dst=100003;rnd=0.5305973063223064.

[14] Ядерный кластер «Сколково» намерен привлечь 1 млрд руб. в 2014 году // РИА НОВОСТИ [сайт]. — М., 18.10.2013. —http://ria.ru/sk_news/20131018/971099036.html.

## References

[1] On science and state scientific and technical policy: Federal Law of the Russian Federation as of August 23, 1996 No. 127-FZ // Sobranie zakonodatel'stva RF. – 1996. – No. 35. – Art. 4137. (In Russ.)

[2] On education in the Russian Federation: Federal Law of the Russian Federation as of December 29, 2012 No. 273-FZ // Sobranie zakonodatel'stva RF. – 2012. – No. 53 (Part 1). – Art. 7598. (In Russ.)

[3] On development of small and mid-sized businesses in the Russian Federation: Federal law as of July 24, 2007 No. 209-FZ // Sobranie zakonodatel'stva RF. – 2007. – No. 31. – Art. 4006. (In Russ.)

[4] On technical regulations: Federal Law as of December 27, 2002 No. 184-FZ // Sobranie zakonodatel'stva RF. – 2002. – No. 52 (Part 1). – Art. 5140. (In Russ.)

[5] On innovation center «Skolkovo»: Federal Law as of September 28, 2010 No. 244-FZ // Sobranie zakonodatel'stva RF. – 2010. – No. 40. – Art. 4970. (In Russ.)

[6] On Federal Law «On innovation activities and state innovation policy»: Resolution of the State Duma of the Federal Assembly of the Russian Federation as of June 21, 2001 No. 1664-III GD (draft № 99029071-2) // Sobranie zakonodatel'stva RF. – 2001. – No. 27. – Art. 2710.

[7] On dismissal of the Federal Law 'On innovation activity and state innovation policy' as of December 1, 1999 passed by the State Duma: Presidential letter as of January 3, 2000 No. Pr-14 [Electronic resource] // Spravochno-pravovaya sistema «Konsul'tantPlyus». http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=4195.

[8] On the establishment of special commission in connection with dismissal of the Federal Law 'On innovation activity and state innovation policy' by the President of the Russian Federation: Resolution of the State Duma of the Federal Assembly of the Russian Federation as of February 18, 2000 No. 93-III GD // Sobranie zakonodatel'stva RF. – 2000. – No. 9. – Art. 1007. (In Russ.)

[9] On the establishment the strategy of innovation development of the Russian Federation for a period of up to 2020: Governmental decree of the Russian Federation as of December 8, 2011 No. 2227-r // Sobranie zakonodatel'stva RF. – 2012. – No. 1. – Art. 216. (In Russ.)

[10] Strategy of development of science and innovations in the Russian Federation in the period of up to 2015: Protocol of Intergovernmental Commission on Scientific and Innovation Policy as of February 15, 2006 No. 1 // Spravochno-pravovaya sistema «Konsul'tantPlyus». - http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=101907;fld=134;dst=100003;rnd=0.5305973063223064

[11] Basic areas of innovation policy in the Russian federation in the period of up to 2010: Resolution of the Government of the Russian Federation as of August 5, 2005 No. 2473p-P7 // Spravochno-pravovaya sistema «Konsul'tantPlyus». http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=91912

[12] Nuclear cluster «Skolkovo» aims at attracting 1 billion rubles in 2014 [Electronic resource] // RIA NOVOSTI.– Moscow, 18.10.2013. –http://ria.ru/sk_news/20131018/971099036.html

[13] On abolition of Governmental Commission on high-tech solutions and innovations: State Resolution of the Russian Federation as of August 16, 2012 No. 839 // Sobranie zakonodatel'stva RF. – 2012. – No. 35. – Art. 4828. (In Russ.)

[14] On Presidential Council of the Russian Federation on modernization of economics and innovation development of Russia: Presidential decree of the Russian Federation as of June 18, 2012 No. 878 // Sobranie zakonodatel'stva RF. – 2012. – No. 26. – Art. 3499. (In Russ.)

---

**Астахова Людмила Викторовна,** д. п. н., профессор, профессор кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: lvastachova@mail.ru

**Иванов Евгений Сергеевич,** аспирант кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: evgeniivan@gmail.com

**Astakhov Ludmila Viktorovna,** PhD Pedagogics, professor, professor of the Department of Information System Security, South Ural State University. E-mail: lvastachova@mail.ru

**Evgueny Ivanov,** post graduate student of the Department of Information System Security, South Ural State University. E-mail: evgeniivan@gmail.com

УДК 004.056.53 + 004.4.056

**Никольская К. Ю.**

# СВОЙСТВА ИНФОРМАЦИИ КАК ОБЪЕКТА ИНФОРМАЦИОННЫХ ПРАВООТНОШЕНИЙ

*Рассмотрено содержание права на информацию и свойства информации как объекта права. Проанализированы нормы конституционного права и действующего законодательства (Конституция Российской Федерации, Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 28.12.2013) «Об информации, информационных технологиях и о защите информации») по вопросам правового регулирования информационных отношений. Сформулированы основные свойства информации, проанализированы юридические особенности основных определений информационного права (информационных процессов, информационных систем, информационных ресурсов, собственника информационных ресурсов, владельца информационных ресурсов, пользователя информации) с точки зрения свойств информации и её защиты в зависимости от категории доступа.*

***Ключевые слова:*** *конфиденциальная информация, право на информацию, свойства информации.*

**Nikolskaya K. Y.**

# FEATURES OF INFORMATION AS AN OBJECT OF INFORMATION RELATIONS

*The author considers the content of the right for information and features of information as an object of law. The rules of constitutional law and legislation (Constitution of the Russian Federation, Federal Law as of 27.07.2006 No. 149-FZ (editorship as of 28.12.2013) "On Information, Information Technologies and Information Security") on legal regulation of information relations are also analyzed. The basic features of information are defined. The article analyzes certain legal aspects of basic definitions of information law (information processes, information systems, information resources, owner of the information resources, the proprietor of the information resources, user of the information) from the viewpoint of properties and information security depending on the type of access.*

***Keywords:*** *confidential information, right for information, features of information.*

Базовым объектом информационного права является информация. Понятие информации имеет много значений. Например, А. А. Стрельцов представляет информацию как результат отражения движения объектов материального мира в системе живой природы. То есть понятие информации не является абстрактным атрибутом материи и проявляется только в жизнедеятельности живых организмов[1].

Информация — сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством, либо сообщения, осведомляющие о положении дел, о состоянии чего-нибудь[2].

Сведения — запечатленные в организме результаты отражения движения объектов материального мира. Они имеют духовный (идеальный, нематериальный) характер, объективны и инвариантны к субъекту восприятия. Предполагается, что сведения не имеют физического носителя, не воспринимаются органами чувств и неуничтожаемы.

Сообщение — набор знаков, с помощью которого сведения передаются другому организму и воспринимаются им. Информация субъективна в виде сообщений, изменяется в процессе восприятия и осознания получателем, а также изменяется в процессе передачи от организма к организму. Сообщения обладают такими свойствами, как материальность (не хранятся без носителя), копируемость и уничтожаемость.

Одной из форм представления информации являются «Данные». Под этим понятием подразумевается представление информации в формализованном виде, пригодном для передачи, обработки или интерпретации. Данные могут обрабатываться автоматическими средствами или людьми[2].

Основными свойствами информации являются:

1. Свойство физической неотчуждаемости информации. То есть знания неотделимы от человека, их носителя. То есть при передаче информации от одного лица к другому и юридическом закреплении этого факта процедура отчуждения информации должна заменяться передачей прав на ее использование и передаваться вместе с этими правами.

2. Свойство обособляемости информации. Информация для осуществления оборота должна овеществляться в виде символов, волн, знаков. После этого она может обособиться от ее создателя (производителя) и существовать независимо от него. Это подтверждает факт оборотоспособности информации как самостоятельного объекта правоотношений, вследствие этого возникает возможность передачи информации от одного субъекта к другому.

3. Свойство информационной вещи (информационного объекта). Это свойство возникает вследствие того, что информация передается и распространяется только на материальном носителе или с помощью материального носителя и проявляется как «двуединство» информации (ее содержания) и носителя, на котором эта информация (содержание) закреплена. Это свойство позволяет распространить на информационную вещь (объект) совместное и взаимосвязанное действие двух институтов — института авторского права и института вещной собственности.

4. Свойство тиражируемости (распространяемости) информации. Информация может распространяться и тиражироваться в неограниченном количестве экземпляров. Одна и та же информация может принадлежать одновременно неограниченному кругу лиц (неограниченный круг лиц может знать содержание этой информации). Следовательно, необходимо юридически закреплять объем прав по использованию информации (ее содержания) лицами, обладающими такой информацией (обладающими знаниями о содержании информации).

5. Свойство организованной формы. Информация, которая находится в обороте, как правило, представляется в документированном виде, т. е. в форме документа. Это могут быть подлинник (оригинал) документа, его копия, массив документов на бумажном или электронном носителе (банк данных или база данных) тоже в виде копии или оригинала, библиотека, архив, фонд документов и т. д. Данное свойство предоставляет возможность юридически закрепить факт «принадлежности» документа конкретному лицу, например, закрепив его соответствующей подписью в традиционном или электронном виде (с помощью ЭЦП). Также это свойство позволяет отнести к информационным объектам (информационным вещам) отдельные документы или сложные организованные информационные структуры.

6. Свойство экземплярности информации. Информация распространяется не сама

по себе, а на материальном носителе, поэтому возможен учет экземпляров информации или учет носителей, содержащих информацию. Данное понятие позволяет учитывать документированную информацию, вследствие чего связывать содержательную сторону информации с ее «вещным» обрамлением, т. е. с отображением на носителе, вводить понятие учитываемой копии документа, а отсюда возникает механизм регистрации информации, в особенности учета обращения оригиналов (подлинников) документов. Экземплярность информации сегодня активно применяется при обращении информации ограниченного доступа.

Указанные юридические особенности и свойства должны учитываться при правовом регулировании информационных отношений.

Научно-технический прогресс превращает информацию в средство активного воздействия на общественное мнение и ценный товар.

Информатизация — это организованный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Информационные процессы — процессы сбора, обработки, накопления, поиска, хранения и распространения информации.

Информационная система — организационно-упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Информационные ресурсы — отдельные массивы документов и документы в информационных системах (архивах, банках данных, библиотеках, фондах и других информационных системах).

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, распоряжения, пользования указанными объектами.

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осуществляющий пользование и владение указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

Пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ей[1].

Право на информацию — одно из основных прав гражданина и человека. Согласно статье девятнадцатой Всеобщей Декларации прав человека, каждый человек имеет право на свободу убеждений и на свободное их выражение. Это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ.

Статья десять Конвенции о защите прав человека и личных свобод гласит, что каждый имеет право свободно выражать свое мнение. Это право включает свободу придерживаться своего мнения и свободу распространять и получать информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ.

Осуществление этих свобод накладывает ответственность и обязанности и сопровождается определенными формальностями, ограничениями, условиями или санкциями, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности, общественного порядка и территориальной целостности, в целях предотвращения преступлений и поддержания правопорядка, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации или обеспечения беспристрастности и авторитета правосудия.

В соответствии с Конституцией Российской Федерации каждому гарантируется право на информацию, то есть право свободно передавать, искать и получать информацию. Право на информацию является неотчуждаемым правом гражданина и человека.

Иностранные граждане и лица без гражданства пользуются в Российской Федерации правом на информацию наравне с гражданами Российской Федерации, кроме случаев, установленных федеральным законом или международным договором Российской Федерации.

Основными принципами реализации права на информацию являются:

• общедоступность и открытость информации;

• обеспечение безопасности личности, общества и государства;

• законность поиска, получения и передачи информации;

• защита права на информацию;

• информированность граждан о деятельности организаций и органов;

• предоставление достоверной информации.

Обеспечение конституционных прав граждан на информационную деятельность, включая право на получение достоверной информации, гарантии возможности свободно получать, искать, производить, передавать и распространять информацию в сочетании с обеспечением свободы слова, свободы прессы и других средств массовой информации является важнейшей составляющей информационной безопасности.

Цензура массовой информации, то есть требование от редакции средства массовой информации со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме случаев, когда должностное лицо является автором или интервьюируемым), а равно наложение запрета на распространение сообщений и материалов, их отдельных частей не допускаются. Создание и финансирование организаций, учреждений, органов или должностей, в задачи либо функции которых входит осуществление цензуры массовой информации, не допускаются.

Категории информации:

1. Общедоступная информация – информация, которая должна предоставляться свободно в силу прямого указания закона в случаях реализации гражданином своих конституционных и иных предоставленных законом прав.

2. Информация ограниченного доступа – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации в целях соблюдения интересов государства или прав и законных интересов их владельцев[2]. К ней относятся государственная тайна, служебная и коммерческая тайны. К этой категории также относят тайны, связанные с правом на неприкосновенность личной жизни: персональные данные, личную и семейную тайны, тайну записи актов гражданского состояния, медицинскую тайну, тайну вероисповедания. Персональные данные – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность. Кроме того, здесь выделяют и группу профессиональных тайн: адвокатскую тайну, нотариальную тайну, журналистскую тайну, тайну исповеди.

**Примечания**

[1] Бачило, И. Л. Информационное право / И. Л. Бачило. — М. : Юрайт, 2012. — 576 с.

[2] Парошин, А. А. Информационная безопасность : стандартизованные термины и понятия / А. А. Парошин. — Владивосток : Изд-во Дальневост. ун-та, 2010. — 216 с.

**References**

[1] I. L. Bachilo. Informatsionnoe pravo [Information law] – Yurait Publ., 2012. – 576 p.

[2] A. A. Paroshin. Informatsionnaya bezopasnost': standartizovannye terminy i ponyatiya [Information security: Standardized terms and notions] - Vladivostok: Dal'nevost. Un-ta Publ., 2010. – 216 p.

**Никольская Ксения Юрьевна,** преподаватель кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: bambucha13@mail.ru

**Ksenia Yurievna Nikolskaya,** lecturer and tutor of the Department of Information System Security of South Ural State University. E-mail: bambucha13@mail.ru

# РЕГИОНАЛЬНЫЙ УЧЕБНО-НАУЧНЫЙ ЦЕНТР «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ЮУрГУ (РУНЦ ИБ ЮУрГУ)

Региональный учебно-научный центр «Информационная безопасность» ЮУрГУ создан при кафедре «Безопасность информационных систем» приборостроительного (компьютерных технологий, управления и радиоэлектроники) факультета во исполнение Приказа Министерства образования и науки Российской Федерации от 9 марта 2005 года № 126 «Об утверждении Перечня региональных учебно-научных центров по проблемам информационной безопасности в системе высшей школы на базе государственных образовательных учреждений высшего профессионального образования, находящихся в ведении Федерального агентства по образованию».

Центр осуществляет повышение квалификации и переподготовку кадров по проблемам информационной безопасности по следующим программам:

**1. Программа профессиональной переподготовки «Комплексные системы обеспечения информационной безопасности в организациях» (504 часа).**

По окончании программы выдается Диплом о профессиональной переподготовке. Потребность в обучении по данной программе обусловлена требованиями Постановления Правительства Российской Федерации от 16 апреля 2012 г. № 313 г. «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)». Центр предлагает пройти обучение по данной программе руководителей и инженерно-технических специалистов подразделений обеспечения информационной безопасности (защиты информации) предприятий, организаций и учреждений.

**Обучение в РУНЦ ИБ ЮУРГУ ведется по модульному принципу с использованием дистанционных технологий.** Слушателям программы профессиональной переподготовки на выбор предлагается 7 из 10 модулей объемом по 72 часа:

КПП-01. Организация и управление системой информационной безопасности организации.

КПП-02. Криптографическая и программно-аппаратная защита информации.

КПП-03. Инженерно-техническая защита информации.

КПП-04. Обеспечение безопасности персональных данных при их обработке в ин-

формационных системах персональных данных.

КПП-05. Расследование инцидентов информационной безопасности.

КПП-06. Документирование защиты информации и организация конфиденциального документооборота.

КПП-07. Защита коммерческой тайны.

КПП-08. Кадровая безопасность.

КПП-09. Культура информационной безопасности.

КПП-10. Криптографическая защита информации.

**2. Программы повышения квалификации** (72 часа). По окончании программ выдается Удостоверение о повышении квалификации.

**2.1. «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных».** Главная цель курса заключается в том, чтобы помочь специалистам различных категорий – от руководителей предприятий и их структурных подразделений до лиц, ответственных за организацию обработки персональных данных, – обеспечить работу с персональными данными в соответствии с требованиями российских законов и с учетом последних изменений в законодательстве. В рамках курса изучается весь комплекс мероприятий по обеспечению правомерности обработки персональных данных с использованием правовых, организационных и технических мер, способы снижения рисков утечки персональных данных и наложения штрафных санкций со стороны государственных надзорных органов.

**2.2. «Защита коммерческой тайны».** В курсе изучаются особенности российского законодательного регулирования вопросов защиты исключительных прав на секреты производства, закрепленные в Федеральном законе от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» и в других нормативных актах, а также технологии установления и поддержания режима коммерческой тайны в организации. Особое внимание уделяется формированию перечня сведений, составляющих коммерческую тайну, разработке и вводу в действие внутренних нормативных документов предприятия, регулированию трудовых отношений, связанных с доступом к коммерческой тайне, процедуре заключения лицензионных договоров, договоров об отчуждении исключительных прав на секреты производства и коммерческой концессии, особенностям представления информации о коммерческой тайне в органы власти, порядку проведения совещаний с контрагентами, на которых раскрывается коммерческая тайна, способам минимизации рисков, вызванных угрозами конфиденциальным сведениям.

**2.3. «Расследование компьютерных инцидентов».** В курсе изучаются все аспекты деятельности службы безопасности (отдела информационной безопасности) организации при реагировании на инциденты в информационной системе, в том числе методика предупреждения таких инцидентов, ликвидации нанесенного ими ущерба, пресечения хакерской активности, перекрытия каналов незаконного съема информации и выявления виновных лиц. Слушатели изучают методики анализа рисков и уязвимостей безопасности информационных систем организации, основные способы обеспечения непрерывности функционирования информационной системы в случае возникновения компьютерных инцидентов и скорейшего устранения их последствий. В завершение курса слушатели самостоятельно проводят полный цикл расследования компьютерных инцидентов с составлением необходимых документов.

**2.4. «Документирование защиты информации и организация конфиденциального делопроизводства».** Цель курса – подготовка слушателей к проведению комплекса мероприятий по защите информации в организации с учетом требований нормативно-правовых документов, регламентирующих защиту информации в организации, в том числе – информации ограниченного доступа и ведения конфиденциального делопроизводства. Особое внимание уделяется практическим аспектам реализации всего процесса конфиденциального делопроизводства – от составления перечня информации ограниченного доступа до особенностей электронного конфиденциального документооборота, использования электронной цифровой подписи. Детально рассматриваются обязанности сотрудников, организующих, осуществляющих и контролирующих конфиденциальное делопроизводство. Специалисты, обучающиеся на курсе, получают практические знания и навыки, позволяющие создать или усовершенствовать существующую систему конфиденциального делопроизвод-

ства на предприятиях и в организациях любой формы собственности и отраслевой принадлежности.

**2.5. «Культура информационной безопасности».** Актуальность программы обусловлена, во-первых, технологизацией образовательного процесса, а следовательно, возрастающими требованиями к развитию компьютерной грамотности руководителя, учителя, специалиста муниципальных образовательных учреждений, во-вторых, существующими тенденциями современного информационного общества, которые повышают зависимость безопасности общества, каждого конкретного человека от качества информационной инфраструктуры, достоверности, целостности используемой информации, ее защищенности от несанкционированной модификации. Обучение направлено на формирование навыков работы с офисными программами и Интернетом, изучение основ защиты информации, а также развитие компетенций в области обеспечения личной информационно-психологической безопасности и защиты детей, подрастающего поколения от негативных информационных воздействий (агрессии, экстремизма, деструктивных организаций, зависимости от информационного шума, сообществ в социальных сетях, провоцирующих суицидальное поведение, и пр.). Программа рассчитана на специалистов образовательных учреждений.

Слушателям предлагаются также курсы повышения квалификации по программам «Программно-аппаратная защита информации», «Криптографическая защита информации», «Инженерно-техническая защита информации» и др.

Кроме образовательной деятельности, Центр активно ведет научные и хоздоговорные исследования по актуальным проблемам защиты информации.

**Контактная информация:**
**Адрес:** 454080, Челябинск, пр. Ленина, 84, ауд. 513/3а.
**Тел.:** 8 (351) 267-99-24, 267-93-77
**E-mail:** runc-ib@mail.ru
**Сайт:** http://runc-ib.susu.ac.ru/

**Contact information:**
**Address:** Office 513/3a, 84 Lenina Str., Chelyabinsk, 454080,
**tel.:** 8(351) 267-99-24, 267-93-77
**E-mail:** runc-ib@mail.ru
http://runc-ib.susu.ac.ru/

**ВЕСТНИК УрФО**
**Безопасность в информационной сфере № 1(11) / 2014**

Подписано в печать 31.03.2014. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 5,60. Тираж 300 экз. Заказ 110/259.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

**Bulletin of the Ural Federal District**
**Security in the Sphere of Information No. 1(11)/2014**

Passed for printing 31.03.2014. Format 70X108 1/16. Screen printing.
Conventional printed sheet 5,60. Circulation - 300 issues. Order 110/259. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080