ISSN 2225-5435

Вестник УрФО

Безопасность в информационной сфере

2/2011

УЧРЕДИТЕЛЬ:
Южно-Уральский государственный университет

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
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 **i-secur@mail.ru**

В номере

Правовой аспект информационной безопасности

М. И. ГРИШАНКОВ
О некоторых проблемах законодательного обеспечения информационной безопасности бизнеса 5
Д. М. ВЕТРОВ
Коммерческая тайна и секрет производства. Новые аспекты законодательства 12

Организация и управление защитой информации

Е. О. ЦАРЕВ, Е. ЛЯШЕНКО
Угрозы информационной безопасности при подготовке и проведении Единого государственного экзамена (ЕГЭ) на уровне субъекта Российской Федерации 17
В. С. КОВАЛЕВ, Т. Ю. ЗЫРЯНОВА
Экспертное оценивание в управлении информационной безопасностью 33

Информационно-психологическая безопасность

Л. В. АСТАХОВА
Информационно-психологическая безопасность в регионе: культурологический аспект 40

Защита информационных систем

А. БОЛГАРСКИЙ
Защита информации в государственных информационных системах 48
М. С. ПОЛИТОВ
Оценка уровня защищённости информационных систем, её достоверность и прогнозирование результатов 51
Д. И. ДИК
Применение мутационного анализа для оценки качества тестирования межсетевых экранов 56
А. Р. ЗАЙНИКАЕВ, А. А. МУРАТОВ, Н. И. СИНАДСКИЙ
Количественная оценка защищенности объектов информационно-телекоммуникационных систем и сетей на основе формирования графов атак с применением перечней уязвимостей и карты сетевой топологии 62
А. А. КОПЫЛОВА, К. А. ПАРШИН
Методика расчета уровня шума в помещении путем расчета звукоизоляции помещения 69

Инженерно-техническая защита информации

Ю. А. МИХАЙЛОВ
Защита информации от утечки по каналам ПЭМИн в современном мире 82

Трибуна молодого ученого

И. И. СУХИХ
Проблемы борьбы с преступлениями в сфере компьютерной информации 84

Практический аспект

Центр по экспортному контролю ЮУрГУ 87

In this issue

Legal Aspect of Information Security

M. I. GRISHANKOV
On some problems related to legislative support of business information security 5
D. M. VETROV
Trade secret and production secret. New legislation aspects 12
E. O. TSAREV, E. LYASHENKO
Threats to information security during preparation for and holding
the Uniform State Examination (EGE) at the level of a constituent entity of the RF 17

Organization of management of information protection

V. S. KOVALEV, T. YU. ZYRYANOVA
Expert assessment in information security management 33

Information-psychological security

L. V. ASTAKHOVA
Information and psychological security in the region: culturological aspect 40

Protection of Information Systems

A. BOLGARSKY
Information protection in state information systems 48
M. S. POLITOV
Estimating security level of information systems, its reliability and results forecasting 51
D. I. DIK
Application of mutation analysis in assessing the quality of fire wall testing 56
A. R. ZAYNIKAEV, A. A. MURATOV, N. I. SINADSKIY
Informational-telecommunicational systems and networks objects security's
quantitative estimate on the basis of forming graphs
of attacks using vulnerabilities lists and network topology map 62
A. A. KOPYLOVA, K. A. PARSHIN
Technique for calculating noise levels in a room by calculating room acoustic isolation 69

Information engineering protection

YU. A. MIKHAILOV
Protection against information outflow via the channel
of the side electromagnetic radiation and aiming in the present-day world 82

Tribune for young scientist

I. I. SUKHIKH
Problems of crime control in the field of computer information 84

The practical aspect

Center for Export Control SUSU 87

ВЕСТНИК УрФО
Безопасность в информационной сфере № 2/2011

Подписано в печать 19.12.2011. Формат 70×108/16. Печать трафаретная.
Усл.-печ. л. 7,35. Тираж 300 экз. Заказ ___.

Отпечатано в типографии ООО «Фотохудожник».
454091, г. Челябинск, ул. Свободы, 155-1.

УДК 346.26 + 334.012.32-027.45 + 005.922.1:346.26
ББК Х401.114 + У290.4-135 + Х711.92

М. И. Гришанков

О некоторых проблемах законодательного обеспечения информационной безопасности бизнеса

M. I. Grishankov

On some problems related to legislative support of business information security

Проблема обеспечения информационной безопасности бизнеса становится сейчас очень острой, особенно с развитием электронного бизнеса. Необходимо грамотно выстраивать как сам бизнес, так и систему его защиты. И эти задачи необходимо решать одновременно. Какие правовые условия для обеспечения информационной безопасности бизнеса существуют и насколько они эффективны, рассматривается в данной статье.

***Ключевые слова**: права на доступ к информации, корпоративные информационные системы и сети, информация ограниченного доступа, внешние угрозы, внутренние угрозы.*

Business information security becomes one of the primary concerns, especially in connection with e-commerce. It is necessary not only to intelligently organize a business, but also to provide its adequate protection. These tasks should be addressed at the same time. This paper covers certain legal prerequisites that must be met to ensure business information safety, and the degree of their efficiency.

***Keywords**: rights of access to information, enterprise information systems and networks, restricted information, external threats, internal threats.*

Мы полагаем, что проблема информационной безопасности бизнеса (далее — ИББ) — комплексная и ее решение требует таких же комплексных подходов.

Исходя из положений Доктрины информационной безопасности Российской Федерации, ИББ можно определить как состояние защищенности от внутренних и внешних угроз интересов субъектов бизнеса в информационной сфере. А их интересы распространяются на три вида объектов:

— информацию, имеющую для конкретного бизнеса коммерческую ценность, и права на нее;

— информационные системы, в которых хранится и обрабатывается такая информация;

— сети связи, по которым она передается.

Защита первых двух объектов, а также защита локальных (корпоративных) сетей связи полностью ложится на плечи предпринимателя, защита сетей связи общего пользования, которыми пользуются предприниматели для передачи информации, — на собственников этих сетей (операторов связи).

Внешние угрозы реализуются в форме недобросовестной конкуренции и промышленного шпионажа.

Правовую базу защиты от внешних угроз ИББ составляют сегодня Федеральный закон № 135-ФЗ «О защите конкуренции» и ряд статей Уголовного кодекса РФ, устанавливающих ответственность за некоторые преступления, которые можно отнести к недобросовестной конкуренции и промышленному шпионажу.

Недобросовестная конкуренция включает, в том числе, такие действия как распространение ложных, неточных или искаженных сведений, которые могут причинить убытки хозяйствующему субъекту либо нанести ущерб его деловой репутации; незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну; незаконное приобретение и использование исключительного права на средства индивидуализации юридического лица, средства индивидуализации продукции, работ или услуг.

Признак недобросовестности — отсутствие согласия на указанные действия со стороны обладателя информации или правообладателя. При этом речь идет не только о разглашении, но и о других действиях с информацией — ее получении и использовании.

Незаконные модификация, блокирование, уничтожение информации — это самостоятельное уголовное преступление, не связанное с недобросовестной конкуренцией.

Внутренние угрозы интересам субъекта бизнеса в информационной сфере реализуются в результате недобросовестности и противозаконной деятельности персонала, а также недостаточно развитой и устойчивой системы обеспечения информационной безопасности. По мнению многих руководителей, внутренние угрозы ИББ представляют для бизнеса наибольшую опасность.

Правовую базу защиты от внутренних угроз составляют, прежде всего, Трудовой кодекс Российской Федерации, Гражданский кодекс Российской Федерации, федеральные законы «О коммерческой тайне», «О персональных данных», «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», «О связи», «Об информации, информационных технологиях и о защите информации», «О лицензировании отдельных видов деятельности», «Об электронной подписи», «О техническом регулировании».

Итак, в целях обеспечения ИББ субъект бизнеса должен организовать защиту следующих объектов:

1) открытой информации, размещаемой на сайте организации;

2) имеющейся в организации информации ограниченного доступа, в том числе информации, составляющей государственную, коммерческую и профессиональные тайны; инсайдерскую информацию, персональные данные;

3) права на доступ к информации, необходимой для ведения бизнеса;

4) корпоративных информационных систем и сетей;

5) объектов интеллектуальной собственности, правообладателем которых является юридическое лицо.

Меры обеспечения ИББ субъект вправе устанавливать самостоятельно в соответствии с российским законодательством, за исключением случаев, когда федеральный закон и принимаемые в соответствии с ним нормативные правовые акты устанавливают обязательные для соблюдения требования. Например, требования по защите сведений, составляющих государственную тайну, требования по защите прав субъектов персональных данных, требования получения лицензии на отдельные виды деятельности, дополнительные требования по обеспечению информационной безопасности, установленные для объектов, оказывающих существенное влияние на безопасность государства в информационной сфере.

Какие правовые условия для обеспечения ИББ существуют и насколько они эффективны? Рассмотрим это для каждого из объектов защиты.

(1) Защита открытой информации, размещенной на сайте организации, — это право организации и ограничения этого права не установлены.

(2) Что касается защиты информации ограниченного доступа, то здесь есть проблемы.

Прежде всего, отсутствует классификация информации ограниченного доступа, а количество видов такой информации уже перевалило за 40. Не установлены общие требования к формированию отдельных правовых режимов ограничения доступа к информации, права и обязанности обладателей информации, ответственность за ее разглашение.

По видам тайн.

Коммерческая тайна. После принятия четвертой части Гражданского кодекса Российской Федерации и внесения изменений в Федеральный закон № 98-ФЗ «О коммерческой тайне» понятие информации, составляющей коммерческую тайну, принципиально изменилось. Если прежде в состав этой

информации могли входить сведения, составляющие секрет производства, то теперь информация, составляющая коммерческую тайну, практически отождествляется со сведениями, составляющими секрет производства (ноу-хау) в смысле статьи 1465 ГК РФ. Что это означает?

В обычаях делового оборота к коммерческой тайне относится, например, информация о потребителях и поставщиках, об условиях договоров поставок и предоставления услуг. Назвать эту информацию «секретом производства» значит исказить смысл этого термина. Но иного способа обеспечить конфиденциальность этой информации нет. Помимо обеспечения конфиденциальности информации, составляющей коммерческую тайну, что является условием защиты ее в этом режиме, руководитель вынужден исполнять все требования оборота этой информации как объекта исключительных прав.

Следует отметить, что проблемы реализации данного федерального закона известны и у ряда экспертов есть предложения по изменению отдельных положений закона и части четвертой Гражданского кодекса. Однако в Государственную Думу соответствующий законопроект не внесен.

Эта ситуация, как ни странно, влияет и на формирование правового института служебной тайны, потому что нужен режим, в котором можно охранять информацию, имеющую коммерческую ценность, но не являющуюся секретом производства.

Служебная тайна. Часть организаций, плотно контактирующих с органами государственной власти, нередко получает документы с пометкой «Для служебного пользования» (ДСП).

Существующий на сегодняшний день порядок работы со служебной информацией определяется Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» и распространяется только на указанные органы.

Правовой режим обращения такой информации вне федеральных органов исполнительной власти законодательно не установлен, хотя данная категория информации (непосредственно или по смыслу) присутствует в большом количестве федеральных законов (около 40).

Базовый для данного законодательства Федеральный закон «Об информации, информационных технологиях и о защите информации» определяет уровень законодательного регулирования — это федеральный закон, устанавливающий условия отнесения информации к сведениям, составляющим служебную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение (ст. 9). Федеральный закон, регулирующий порядок установления режима служебной тайны, не принят и ответственность не установлена.

С 2004 года в Государственной Думе находился на рассмотрении проект федерального закона «О служебной тайне», внесенный группой депутатов, включая меня. Однако рассмотрения как такового не было. Вначале мы дорабатывали проект по замечаниям органов государственной власти, внесли новую редакцию в 2006 году. И с тех пор нам не удавалось преодолеть позицию правительства, которое считает, что реализация федерального закона потребует бюджетных затрат на техническую защиту информации, составляющей служебную тайну.

Мы считаем, что эта позиция спорна, потому что сейчас документы с пометкой «ДСП» широко используются и защищаются в органах государственной власти из имеющихся средств. Для нас очевидно, что практика широкого использования такой пометки в документах органов государственной власти всех уровней, в том числе направляемых в государственные и негосударственные организации, требует правового регулирования на уровне федерального закона (включая доступ к такой информации, ее передачу, хранение и уничтожение), а также установление ответственности за ее разглашение.

Вместе с тем, за прошедшие 5 лет было принято несколько федеральных законов, влияющих на концепцию рассматриваемого законопроекта (это введение в действие части четвертой Гражданского кодекса, федеральные законы о персональных данных и об использовании инсайдерской информации).

В связи с этим Комитетом Государственной Думы по безопасности было принято решение снять законопроект с рассмотрения через отклонение при рассмотрении его в первом чтении. Будем работать над новой концепцией законопроекта[1].

Профессиональная тайна. Обязанность по защите профессиональной тайны и состав защищаемой информации проистекают из специальных законов, в том числе: законов о связи, о частной охранной и детективной деятельности, о нотариате, об охране здоровья граждан, банковской дея-

тельности, об адвокатской деятельности и многих других.

Анализ содержания сведений, составляющих профессиональную тайну, свидетельствует о том, что в этом режиме охраняются, как правило, персональные данные и информация, составляющая коммерческую тайну, доверенные специалисту в рамках его профессиональной деятельности.

Однако общих требований по безопасности информации, составляющей профессиональную тайну, нет, за исключением требований обеспечения ее конфиденциальности, требований закона об обеспечении безопасности персональных данных при их обработке и общих положений о защите информации, предусмотренных Федеральным законом «Об информации…».

Инсайдерская информация. Перечень инсайдерской информации установлен приказом Федеральной службы по финансовым рынкам от 12 мая 2011 г. и занимает 22 страницы. Интересно, что в состав инсайдерской информации может входить и информация, составляющая коммерческую, служебную, банковскую, налоговую и иную тайну.

Вместе с тем, в соответствии с законом, данный вид информации не является априори информацией ограниченного доступа (это временный режим). Закон устанавливает условия, при которых использование такой информации правомерно. Более того, законом установлены требования по раскрытию такой информации в определенных случаях. Однако юридические лица обязаны принять меры по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации.

За неправомерное использование инсайдерской информации установлена уголовная (ст. 185.6 УК РФ) и административная ответственность (ст. 15.21 КоАП РФ).

При этом закон не устанавливает требования к порядку защиты инсайдерской информации, за исключением отсылки к законодательству о государственной тайне и о налогах и сборах. В связи с чем возникает вопрос о мерах защиты инсайдерской информации, которые в случае ее неправомерного использования будут признаны судом достаточными.

Персональные данные. Вопросы совершенствования законодательства о персональных данных и анализа проблем правоприменения были в центре внимания последние года три, поэтому нет необходимости особенно это комментировать. В последней версии федерального закона было учтено большинство предложений операторов информационных систем персональных данных, за исключением положений по обеспечению безопасности персональных данных и правовых режимов конфиденциальности персональных данных. Несмотря на концепцию совершенствования закона, выработанную на парламентских слушаниях, в окончательном тексте получила закрепление позиция правительства по данному вопросу. Жизнь покажет эффективность этих решений.

Тем не менее, ментальность наша начала меняться: и граждане стали внимательнее относиться к своим данным, и операторы учатся их защищать. Этот процесс в Европе занял не менее 10 лет. Мы пока в середине пути.

Проблема защиты персональных данных обостряется для тех, кто ведет электронный бизнес. Электронные магазины до сих пор собирают избыточную информацию о клиентах. Например, если товар доставляется по месту работы, зачем требовать домашний адрес? Да и к защите клиентских баз еще относятся недостаточно серьезно. Примерами тому недавние утечки данных, накапливаемых операторами связи.

Целям обеспечения ИББ служит и электронная подпись. В связи с расширением использования информационных технологий для ведения бизнеса (подготовка и заключение договоров в электронном виде, проведение электронных платежей, электронные торги и т. п.) остро встают вопросы защиты передаваемой информации от модификации, копирования и уничтожения, а также обеспечение неизменяемости маршрута сообщений и аутентификации адресата. Определенный вклад в решение этих задач может внести использование технологий электронной подписи.

Федеральный закон № 63-ФЗ «Об электронной подписи», принятый в апреле текущего года, позволил сделать шаг вперед в использовании электронных подписей разного вида.

Вместе с тем, в законе не решен главный вопрос: сферы допустимого и обязательного использования электронной подписи разных видов. Требования к электронной подписи должны быть включены в федеральные законы, предусматривающие использование таких подписей в различных правоотношениях. Такой подход имеет право на жизнь, и он реализован во втором принятом Федеральном законе № 65-ФЗ, предусматривающем внесение изменений в связи с принятием Федерального закона «Об электронной подписи», однако этим законом изменения

внесены в 6 федеральных законов, а следует их внести как минимум еще в 28.

Остались недостаточно определенными: правовой статус подписи юридического лица; права, обязанности и ответственность подписывающего лица и лица, принимающего подпись; процедуры проверки ЭП (в том числе проверки вида ЭП); условия и правовые последствия использования средств ЭП в автоматическом режиме. Не предусмотрена разработка технических требований к сервисам, предоставляемым УЦ.

Так что работы впереди еще много.

(3) Следующий объект защиты — право на доступ к информации, необходимой для ведения бизнеса. Реализация этого права осуществляется в рамках федеральных законов № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» и № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации». Эти законы закрепляют права юридических лиц на доступ к соответствующей информации.

Но немаловажное значение имеют условия доступа: платность, форма представления информации. В частности, мы с вами были свидетелями спора по поводу платности услуг Ростехрегулирования по предоставлению текстов национальных стандартов. Интересы общества отстаивал Институт развития свободы информации. Точку в этом споре поставил Верховный Суд, который своим решением от 2 февраля 2010 года фактически признал правомерным предоставление за плату текстов национальных стандартов. Справедливости ради надо сказать, что новые стандарты размещаются на сайте Ростехрегулирования в формате PDF. Однако там же присутствует предупреждение, что эти тексты «не подлежат копированию, тиражированию и дальнейшему распространению». Понятно, что такая услуга позволяет только ознакомиться с документом и принять решение о целесообразности его приобретения за плату.

Необходимо отметить, что в целях обеспечения безопасности бизнеса, в том числе информационной безопасности, часто требуется проверка персональных данных принимаемых на работу лиц, в том числе документов об образовании. Полагаем, что организацию предоставления такой очень востребованной услуги может взять на себя Минобрнауки, для чего надо только создать федеральный банк таких документов.

Аналогичную услугу юридическим лицам может оказывать МВД России по проверке паспортных данных, тем более, что база данных там уже создана. При этом вполне возможно организовать предоставление информации таким образом, чтобы оно не нарушало требования Федерального закона № 152-ФЗ «О персональных данных».

(4) Защита локальных (корпоративных) компьютерных систем и сетей осуществляется собственниками этих объектов самостоятельно или с привлечением специализированных организаций. Правовую основу этой деятельности составляет Федеральный закон №126-ФЗ «О связи».

(5) Защита объектов интеллектуальной собственности, правообладателем которых является организация, осуществляется в соответствии с положениями части четвертой Гражданского кодекса Российской Федерации.

Особую проблему в этой связи представляют участившиеся нарушения интеллектуальных прав в Интернете, в том числе авторских прав на дизайн и принципы организации корпоративных сайтов. Защита авторских прав, нарушаемых с использованием Интернета, представляет собой глобальную проблему в силу трансграничности Сети. Вместе с тем, в рамках юрисдикции России наше законодательство позволяет защищать эти права.

Обеспечивая информационную безопасность бизнеса, необходимо учитывать установленные законом ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации[2].

В связи с этим необходимо обратить внимание на использование специальных технических средств, предназначенных для негласного получения информации (СТС). Эти средства в последнее время получили развитие и широко используются в бизнесе как в целях недобросовестной конкуренции, так и в целях защиты от нее.

Свободное использование таких технических средств[3] физическими и юридическими лицами запрещается Федеральным законом № 144-ФЗ «Об оперативно-розыскной деятельности». Этим же законом ограничивается разработка, производство, реализация и приобретение в целях продажи СТС индивидуальными предпринимателями и юридическими лицами, а также установлен особый порядок ввоза в Российскую Федерацию и вывоз за ее пределы указанных технических средств (только по лицензии).

Установлена уголовная ответственность за незаконные производство, сбыт или приобретение СТС, за нарушение тайны пере-

писки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан с использованием СТС (ст. 138 УК РФ).

Предусмотрена и административная ответственность за нарушение правил производства, хранения, продажи и приобретения СТС (ст. 20.23. КоАП РФ). Эти положения законодательства надо знать и учитывать при формировании систем ИББ.

Как уже упоминалось ранее, государством могут быть установлены для отдельных объектов дополнительные требования по обеспечению информационной безопасности.

В рамках полномочий ФСТЭК России выделена функция обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере (так называемые ключевые системы информационной инфраструктуры). Это информационные системы, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям. Такие системы могут функционировать, в том числе, в составе критически важных объектов.

Анализ законодательства свидетельствует о том, что объектный состав ключевых систем информационной инфраструктуры и состав критически важных объектов Российской Федерации могут различаться. При этом, если состав критически важных объектов определен секретными Постановлениями Правительства РФ, то состав ключевых систем информационной инфраструктуры и требования к таким системам законодательно не установлены. Таким образом, имеет место неопределенность объектов защиты, нарушение безопасности которых угрожает национальной безопасности.

В рамках указанных полномочий ФСТЭК России утвердил в 2007 году ряд документов методического характера, имеющих гриф «ДСП», которые стимулируют бизнес-субъекты к дополнительным капиталовложениям. Такое положение дел, по нашему мнению, не вполне соответствует конституционным принципам и условиям ограничения прав и свобод человека и гражданина.

Представляется более правильным исходить из необходимости обеспечения комплексной безопасности критически важных объектов, включая защиту информационных и телекоммуникационных систем этих объектов.

К числу критически важных объектов относятся, в том числе, негосударственные организации, вынужденные самостоятельно финансировать создание, поддержание и развитие системы комплексной безопасности. Требования к таким организациям, их права, полномочия органов государственной власти в отношении деятельности этих организаций должны быть установлены отдельным федеральным законом.

Что касается антитеррористической защищенности объектов, то соответствующий законопроект внесен в Государственную Думу и принят в первом чтении в мае этого года[4]. Понятно, что подготовка этого законопроекта стимулирована террористическими актами на объектах транспортной инфраструктуры.

В заключение хочу подчеркнуть следующее: в целом безопасность бизнеса — это комплексная проблема, и неверно сосредотачиваться на вопросах информационной безопасности, игнорируя, например, вопросы пожарной безопасности, поскольку информационные системы организации могут выйти из строя не только из-за DDos-атак или вирусов, компьютеры могут просто сгореть.

Проблема обеспечения информационной безопасности бизнеса становится сейчас очень острой, особенно с развитием электронного бизнеса. Решение проблемы достаточно затратно. Оптимизировать эти затраты можно только грамотно выстроив как сам бизнес, так и систему его защиты. Причем жизнь доказывает: если построение этих систем идет параллельно или последовательно (на сложившуюся систему бизнеса «навешивается» система безопасности) — собственник проигрывает. Эти задачи необходимо решать одновременно.

Примечания

[1] Интересующихся этой проблемой отошлю к нашей с Еленой Константиновной Волчинской статье в журнале «Государственная служба», № 2, 2011 год.

[2] Это определено Федеральным законом «Об информации…» (ст. 16).

[3] К таким средствам относятся (согласно Постановлению Правительства от 01.07.96 № 770):

1. Специальные технические средства для негласного получения и регистрации акустической информации.
2. Специальные технические средства для негласного визуального наблюдения и документирования.

3. Специальные технические средства для негласного прослушивания телефонных переговоров.
4. Специальные технические средства для негласного перехвата и регистрации информации с технических каналов связи.
5. Специальные технические средства для негласного контроля почтовых сообщений и отправлений.
6. Специальные технические средства для негласного исследования предметов и документов.
7. Специальные технические средства для негласного проникновения и обследования помещений, транспортных средств и других объектов.
8. Специальные технические средства для негласного контроля за перемещением транспортных средств и других объектов.
9. Специальные технические средства для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.
10. Специальные технические средства для негласной идентификации личности.

[4] Законопроект № 534519-5 «О внесении изменений в Федеральный закон «О противодействии терроризму» и Федеральный закон «О транспортной безопасности».

ГРИШАНКОВ Михаил Игнатьевич, первый заместитель председателя Комитета Госдумы РФ по безопасности.

GRISHANKOV Mikhail Ignatievich, First Deputy Chairman of the Defense Committee of RF State Duma.

УДК 347.77.023 + 005.922.1
ББК Х404.022 +Х404.3

Д. М. Ветров

Коммерческая тайна и секрет производства. Новые аспекты законодательства

D. M. Vetrov

Trade secret and production secret. New legislation aspects

В статье рассматриваются законодательные аспекты и понятие коммерческой тайны, объединяющей в себе секрет производства (ноу-хау) и коммерческую информацию как об объекте, относящемся к нетрадиционным объектам интеллектуальной собственности.

***Ключевые слова**: рынок информации, секрет производства, коммерческая тайна, ноу-хау.*

The paper provides an overview of legislative aspects and the concept of a trade secret comprising a production secret (know-how) and commercial information, as an non-traditional object of intellectual property.

***Keywords**: Information market, production secret, trade (commercial) secret, know-how.*

С развитием гражданского оборота и информационных технологий возрастает необходимость обеспечить секретность различных сведений в предпринимательской деятельности. Обеспечение секретности сведений в деятельности юридического лица связано с установлением режима коммерческой тайны в отношении сведений, которые ранее было принято называть «конфиденциальная информация».

Нормами законодательства правовая охрана в качестве объекта интеллектуальной собственности предоставляется секретам производства (ноу-хау). К ним относятся сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также информация о способах ведения профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны (ст. 1465 ГК РФ).

С 1 января 2008 г. в Федеральный закон № 98-ФЗ «О коммерческой тайне» (далее — Закон о коммерческой тайне) были внесены изменения, в результате которых предметом его регулирования остались лишь отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау), а в рамках ст. 128 Гражданского кодекса РФ информация исключена из числа самостоятельных объектов гражданских прав, и это в полной мере касается части информации, составляющей коммерческую тайну, являющейся объектом защиты со стороны ее правообладателей. Хотя в различных значениях она продолжает оставаться объектом гражданских правоотношений с определенными свойствами товара.

Рынок информации начинает доминировать в российской экономике, догоняя энергетический рынок[1]. Уже никто не отрицает, что информационные отношения представляют собой новый вид общественных отношений[2], а информация является весьма ценным товаром[3].

Таким образом, сегодня практический интерес представляет вопрос о соотношении и возможном взаимном поглощении понятий «секрет производства» и «коммерческая тайна». При этом безусловно доминирующей

будет являться дискуссия о возможности установления режима коммерческой тайны в отношении любой конфиденциальной информации, поскольку главной целью введения режима коммерческой тайны является получение любых преимуществ, дохода, прибыли обладателем такой информации или режим коммерческой тайны может быть установлен только в отношении информации, составляющей секрет производства в рамках понятия, определенного ст. 1465 Гражданского кодекса РФ?

В литературе продолжает обсуждаться вопрос о правовой природе понятия «информация» несмотря на факт ее исключения из числа объектов гражданского права. Обоснованно подчеркивается необходимость учета связи информации с материальным носителем, на котором она отображена. Большинство ученых-юристов применительно к обороту информации отмечают, что она не может быть объектом правоотношений безотносительно к ее материальным носителям[4]. Правовое значение этой связи установил В. А. Дозорцев, который подчеркивал, что информация должна быть зафиксирована на материальном носителе так, чтобы ее можно было идентифицировать в случае нарушения права на коммерческую тайну[5]. По этому пути идет и законодатель, который ввел понятие документированной информации, т. е. информации, закрепленной на материальном носителе, только такая информация признается объектом прав и может быть предметом договора передачи другому субъекту (п. 6 ст. 3 Закона о коммерческой тайне).

Режим коммерческой тайны считается установленным, если в отношении секретных сведений их обладателем были предприняты меры, предусмотренные ст. 10 Закона № 98-ФЗ. Примечательно, что ни само ноу-хау как объект правовой охраны, ни исключительные права на него не требуют предварительной регистрации. Соответственно отсутствует какой-либо охранный документ, подтверждающий права обладателя на определенные сведения, равно как и перечень охраняемых сведений. Возникновение, существование и прекращение секрета производства и исключительных прав на него зависят только от волеизъявления и распорядительных действий правообладателя.

Носитель документированной информации согласно ГОСТу Р51141-98 «Делопроизводство и архивное дело. Термины и определения» (утвержден постановлением Госстандарта РФ № 28 от 27.02.1998 г.) — это материальный объект, который используется для закрепления хранения на нем речевой, звуковой или изобразительной информации, в том числе в преобразованном виде. В число названных материальных объектов входят рукописные, машинописные, кино-, фото-, фонодокументы, изобразительные документы (документы, содержащие информацию, выраженную посредством изображения какого-либо предмета), документы на машинном носителе, созданные с использованием носителей и способов записи, обеспечивающих обработку информации электронно-вычислительной машиной.

Р. В. Северин выделяет следующие свойства, характеризующие информацию как товар[6].

Во-первых, это потребительские свойства. Речь идет не просто о документах, хранящихся в организации и соответствующих направлениям ее деятельности, а о специально подобранных и систематизированных сведениях, необходимых для решения конкретных производственных задач в целях получения дохода.

Во-вторых, важнейшим свойством информации как товара является ее цена. Формирование цены на информационные продукты (услуги) — это результат анализа рентабельности возможного использования предлагаемой к продаже информации и конъюнктуры информационного рынка. Факторами, влияющими на установление цены, являются затраты на разработку информационного продукта, качество представленной информации, ожидаемый спрос на предлагаемый информационный продукт, уровень ожидаемой прибыли от использования информации.

В-третьих, ценность информации поразному проявляется на различных фазах жизненного цикла продукции, технологии и товара в процессе инновационной деятельности, направленной на освоение новшества[7], содержанием которого чаще всего является не изобретение, а информация, составляющая коммерческую тайну (ноу-хау).

В статье 1465 ГК РФ раскрыто понятие секрета производства (ноу-хау), которое полностью воспроизведено в п. 2 ст. 3 Закона о коммерческой тайне для целей определения уже другого понятия — информация, составляющая коммерческую тайну (секрет производства). Такой подход указывает на то, что законодатель не различает эти понятия, рассматривает их как единое правовое явление, наделяя одними и теми же признаками охраноспособности[8]. При этом коммерческая тайна упоминается в главе 75 ГК

РФ лишь в связи с установлением правового режима.

Говоря о соотношении секрета производства (ноу-хау) и понятия коммерческой тайны в структуре гражданского законодательства, нужно отметить их различную роль в производстве продукции и реализации товаров. Следует согласиться с мнением тех ученых, которые считают, что понятие коммерческой тайны существенно шире, чем понятие «ноу-хау», так как коммерческую тайну могут составлять также списки клиентов, первичные бухгалтерские документы, биржевая и финансовая информация о рынке товаров и капиталов, коммерческих сделках и другие сведения[9]. В Законе о коммерческой тайне и в части четвертой ГК РФ эту проблему можно решить путем увязки понятий секрета производства (ноу-хау) и конфиденциальной информации при определении коммерческой тайны, с одной стороны, и отнесения их к объектам интеллектуальной собственности — с другой.

Если допустить различный объем понятийного аппарата «коммерческая тайна» и «секрет производства», обоснованным представляется законодательное допущение возможности включения в договор различных форм ответственности за нарушение режима конфиденциальности ноу-хау, например в виде штрафа, размер которого, будучи закрепленным в соглашении сторон, не подлежит доказыванию в отличие от размера причиненных убытков[10], в то время как подобная конструкция договора в отношении разглашения содержания регистров бухгалтерского учета невозможна и сторона, доказывающая факт разглашения информации, юридически составляющей коммерческую тайну, будет вынуждена доказывать наличие факта причиненных убытков от ее разглашения в суде.

Также следует обратить внимание на еще одно отличие ноу-хау от ранее употребляемого понятия «информация, составляющая коммерческую тайну» — при создании ноу-хау внутри организации за счет сил сотрудников организации объект принимается организацией к бухгалтерскому учету в качестве актива конкретного вида (нематериального актива), если он отвечает определению данного вида актива и выполняются условия, установленные соответствующим положением по бухгалтерскому учету.

В настоящее время бухгалтерский учет нематериальных активов урегулирован Положением по бухгалтерскому учету «Учет нематериальных активов»[11]. В соответствии со ст. 4 указанного положения секрет производства отнесен к нематериальным активам. Однако в рассмотренном положении нет четкого указания на возможность отнесения к нематериальным активам коммерческой тайны. Если исходить из положения об идентичности понятий, тогда вопрос отпадает сам собой, но если все же предположить, что понятие «коммерческая тайна» шире понятия «секрет производства», то вопрос остается нераскрытым.

Интересный момент отмечает д-р юрид. наук В. Н. Лопатин[12]. Коммерческая тайна в настоящее время идентифицируется с секретами производства (ноу-хау), а в п. 1 ст. 6 «Предоставление информации, составляющей коммерческую тайну» Закона № 98-ФЗ говорится: «Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну», поэтому в соответствии с существующим ныне законодательством обладатель ноу-хау будет обязан безвозмездно предоставлять свои секреты производства в соответствующие организации на материальном носителе, при этом должен быть нанесен гриф «Коммерческая тайна» с указанием обладателя этой информации.

При досконально анализе ст. 1466, 1467 Гражданского кодекса РФ следует предположить, что исключительное право использования и распоряжения данных, составляющих секрет производства, обладатель получает с момента введения режима коммерческой тайны. Законодатель почему-то не наделяет обладателя информации, подпадающей под признаки результата интеллектуальной деятельности и составляющей коммерческую тайну, исключительным правом ее использования и распоряжения с момента введения режима коммерческой тайны, а закрепляет это право только за обладателем секрета производства. Таким образом, если допускать, что понятие «коммерческая тайна» включает в себя не только секрет производства, то у обладателя коммерческой тайны, не относящейся к секрету производства, не существует абсолютной защиты на основании закона. Хотя как в первом, так и во втором случае защита основана на обеспечении конфиденциальности, а ее утрата влечет прекращение прав (ст. 1467 ГК РФ)[13].

Объединяющим признаком секрета производства (ноу-хау) и коммерческой тайны является коммерческая ценность составляющих их сведений, необщеизвестность

и необщедоступность которых позволяют правообладателю путем введения режима коммерческой тайны получать прибыль от оборота такой информации.

Механизм традиционных исключительных прав связан с результатом интеллектуальной деятельности, а механизм защиты коммерческой тайны — с конфиденциальностью сведений, охраняемых в режиме коммерческой тайны[14].

В случае нарушения традиционных исключительных прав объект интеллектуальной собственности не исчезает, тогда как при утрате конфиденциальности соответствующих сведений исключительное право на секрет производства прекращается у всех правообладателей (ст. 1467 ГК РФ). Следует согласиться с З. Ф. Гайнуллиной в том, что права на коммерческую тайну по сути своей исключительные и строятся по модели исключительных прав на ноу-хау[15]. Однако в части четвертой ГК РФ речь идет только о секрете производства (ноу-хау), а не о коммерческой тайне как объекте интеллектуальной собственности. Поэтому при условии внесения изменений в гражданское законодательство информацию, составляющую коммерческую тайну, можно будет относить к объектам интеллектуальной собственности, а права обладателя коммерческой тайны рассматривать в качестве исключительных.

Если рассматривать вслед за В. А. Дозорцевым секрет производства (ноу-хау) как компонент коммерческой тайны[16], то доводы о том, что коммерческую тайну нельзя относить к объектам интеллектуальной собственности, окажутся лишенными всякой логики. Справедливым представляется мнение А. П. Сергеева о том, что фактическая монополия, лежащая в основе коммерческой тайны, и такой признак интеллектуальной собственности, как результат интеллектуальной деятельности, позволяют отнести ее к объектам интеллектуальной собственности, хотя и с рядом специфических особенностей[17].

На наш взгляд, следует согласиться с точкой зрения Р. В. Северина[18]. Представляется, что определение коммерческой тайны как «режима конфиденциальности информации» противоречит содержанию ст. 1465 ГК РФ, закрепившей условия предоставления охраны сведениям, составляющим секрет производства (ноу-хау). Статья 139 ГК РФ содержала такое условие охраны: «…Обладатель информации, составляющей коммерческую тайну, принимает меры к охране ее конфиденциальности». Оно было заменено следующим условием: «…Обладателем таких сведений введен режим коммерческой тайны» (ст. 1465 ГК РФ).

Таким образом, определяя понятие коммерческой тайны через режим конфиденциальности информации, законодатель, по существу, отождествляет меры, направленные на охрану конфиденциальности, с режимом коммерческой тайны, что не одно и то же. В прежней редакции п. 3 ст. 3 Закона о коммерческой тайне режим коммерческой тайны определялся как «правовые, организационные, технические и иные меры по охране конфиденциальности». Однако в ст. 1465 ГК РФ уже говорится не о «мерах по охране конфиденциальности информации», а о сведениях, в отношении которых обладателем введен режим коммерческой тайны, причем в ГК РФ данный термин не раскрывается. Исключение из текста Закона о коммерческой тайне основного понятия «режим коммерческой тайны» осложняет его понимание, напрямую связанное с охраной конфиденциальности информации (ст. 10).

В настоящее время можно говорить о коммерческой тайне, объединяющей в себе секрет производства (ноу-хау) и коммерческую информацию, как об объекте, относящемся к нетрадиционным объектам интеллектуальной собственности, требующим своего окончательного законодательного урегулирования.

Примечания

[1] См.: Информационные системы и технологии в экономике и управлении : учебник / под ред. В. В. Трофимова. — М., 2007. — С. 7—23.
[2] См.: Право и информатика / под ред. Е. А. Суханова. — М., 1990. — С. 6—7.
[3] См.: Гражданское право : учебник / отв. ред. Е. А. Суханов. — М., 2000. — Т. 2. — Полут. 1. — С. 563—635; *Пугинский Б. И.* Коммерческое право России : учебник. — М., 2006. — С. 247—251.
[4] См., напр.: *Бачило И. Л.* Информационное право: основы практической информатики : учебное пособие. — М., 2003. — С. 61—71; *Гаврилов О. А.* Информатизация правовой системы России. Теоретические и практические проблемы. — М., 1998. — С. 8—19; *Снытников А.А.* Информация как объект гражданских правовых отношений : автореф. дис. … канд. юрид. наук. — Тверь ; СПб., 2000; *Шевердяев С. Н.* Проблемы конституционно-правового регулирования информационных отношений в Российской Федерации : автореф. дис. … канд. юрид. наук. — М., 2002.

[5] См.: *Дозорцев В. А.* Интеллектуальные права: Понятие. Система. Задачи кодификации. — М., 2005. — С. 249.
[6] См.: *Северин Р. В.* Объект коммерческой тайны: понятие и признаки // Законодательство. — 2009. — № 11. — С. 40.
[7] См.: *Устинов В. А.* Управление инновационной деятельностью в процессе создания новой техники, освоения новой продукции. — М., 1995. — С. 37—56; *Фатхутдинов Р. А.* Инновационный менеджмент. — М., 2000. — С. 24—89.
[8] *Северин Р. В.* Указ. соч.
[9] См.: *Козырев А. И.* Оценка интеллектуальной собственности. — М., 1997. — С. 21.; *Северин Р. В.* Указ. соч. — С. 41.
[10] *Яковлева О. А.* Коммерческая тайна по-новому // Финансовые и бухгалтерские консультации. — 2009. — № 4. — С. 15.
[11] Положение о бухгалтерском учете 14/2007. Утверждено Приказом Министерства финансов РФ № 153н от 27.12.2007 г. // Российская газета. — 2008. — 2 февр.
[12] *Лопатин В. Н.* Правовые условия и экономические последствия изменения законодательства о коммерческой тайне // Вопросы совершенствования законодательства в сфере обеспечения информационной безопасности. — М. : Изд. Государственной Думы, 2007. — С. 35.
[13] См.: *Северин Р. В.* Указ. соч. — С. 39.
[14] *Шерстобитов А. Е.* Исключительное право на секрет производства («ноу-хау») // Разработка правовых механизмов инновационного развития российского государства / под ред. С. А. Авакьяна. — М., 2008. — С. 108.
[15] См.: *Гайнуллина З. Ф.* Правовое обеспечение прав и законных интересов обладателей необщедоступной информации (коммерческой тайны, ноу-хау) : автореф. дис. … канд. юрид. наук. — М., 1998. — С. 10, 19.
[16] См.: *Дозорцев В. А.* Указ. соч. — С. 250.
[17] См.: *Сергеев А. П.* Право интеллектуальной собственности в Российской Федерации : учебник. — М., 2004. — С. 675, 676.
[18] См.: *Северин Р. В.* Указ. соч. — С. 41.

Д. М. ВЕТРОВ, к. ю. н., доцент кафедры гражданского права и гражданского процесса ЧелГУ.

D. M. VETROV, Candidate of Legal Sciences, the Chair of Civil Law and Civil Procedure.

УДК 371.27:004.056(440)
ББК Ч421.28(2) + Ч401.121(2)

Е. О. Царев, Е. Ляшенко

Угрозы информационной безопасности при подготовке и проведении Единого государственного экзамена (ЕГЭ) на уровне субъекта Российской Федерации

E. O. Tsarev, E. Lyashenko

Threats to information security during preparation for and holding the Uniform State Examination (EGE) at the level of a constituent entity of the RF

В статье охарактеризована информационная модель процесса подготовки и проведения ЕГЭ, предпринят анализ угроз этому процессу, выявлены наиболее вероятные угрозы. В процессе анализа прав доступа и обязанностей лиц, задействованных в подготовке и проведении ЕГЭ, были выделены лица и группы лиц, уровень возможностей которых достаточен для фальсификации результатов. Путем расчетов было получено количество фальсифицированных работ, необходимое для того, чтобы результаты ЕГЭ можно было считать достоверными.

***Ключевые слова**: ЕГЭ, угрозы, информационная безопасность, модель нарушителя, субъект Российской Федерации.*

The paper describes an information model of the process of preparation for and holding the Uniform State Examination (EGE), analyses certain related threats and identifies the most likely threats. Analysis of the access rights and duties of persons involved in EGE preparation and holding helps define certain persons and group of persons having sufficient authorities to falsify the exam results. The authors have also calculated a number of falsified papers that are sufficient to consider EGE results as statistically reliable.

***Keywords**: EGE, threats, information security, violator's model, constituent entity of the Russian Federation.*

В последние годы в Российской Федерации государственными органами управления образованием и образовательными учреждениями различного уровня проводятся мероприятия и эксперименты по диагностике качества образования. К таковым можно отнести введение Единого государственного экзамена (ЕГЭ), для чего созданы банки контролирующих материалов, аппаратно-программные комплексы компьютерного и бланочного тестирования, методики экспертизы качества контролирующих материалов, методики шкалирования и анализа результатов, подходы к интерпретации результатов при принятии управленческих решений.

В процессе подготовки и проведения ЕГЭ участвуют:

1. Федеральный институт педагогических исследований (ФИПИ) формирует набор контрольно-измерительных материалов (КИМ; набор заданий) и передает их в центр тестирования (ЦТ).

2. Центр тестирования (ЦТ) тиражирует КИМ, формирует пакеты и передает в орган управления образованием Российской Федерации (ОУО РФ); создает матрицы ответов; обрабатывает результаты экзамена.
3. Федеральная база свидетельств (ФБС) — организация, предназначенная для хранения и освидетельствования аттестатов.
4. Московский институт экономики и математики (МИЭМ) отвечает за корректную работу ФБС.
5. Рособрнадзор — Федеральная служба по надзору в сфере образования и науки в РФ осуществляет контроль за качеством образования.
6. Орган управления образованием Российской Федерации (ОУО РФ), в чьи задачи входят руководство деятельностью муниципального органа управления образованием (МОУО); создание дочерней организации — регионального центра обработки информации (РЦОИ); обеспечение РЦОИ материально-техническими средствами; создание условий для проведения ЕГЭ (место проведения с соответствующей материально-технической базой); передача КИМ в РЦОИ.
7. Региональный центр обработки информации (РЦОИ) отвечает за обучение и подготовку квалифицированных кадров для проведения ЕГЭ (эксперты), распределяет КИМ по пунктам проведения экзамена; производит сбор всей информации из пункта проведения экзамена (ППЭ) и пункта предварительной обработки информации (ППОИ); производит предварительную обработку результатов экзамена и передает их ЦТ.
8. Муниципальный орган управления образованием (МОУО) отвечает за формирование и подготовку пункта предварительной обработки информации (ППОИ); формирование и организацию работ пункта проведения экзамена (ППЭ).
9. Первичный пункт обработки информации (ППОИ) — это пункт, в котором производится сбор данных об учащихся, формирование их рассадки, а также печать бланков ответов. Создаются, как правило, несколько ППОИ. Информация из ППОИ доставляется в РЦОИ.
10. Пункт проведения экзамена (ППЭ) — это место (как правило, учебное заведение — школа, лицей) для проведения ЕГЭ, в котором одновременно собраны выпускники из нескольких близлежащих школ.

Информация, участвующая в процессе проведения Единого государственного экзамена (ЕГЭ), может быть условно разделена на несколько типов: экзаменационные материалы (КИМ); экзаменационные бланки; результаты экзамена; информация о рассадке, вариантах КИМ; служебная информация (приказы, распоряжения, нормативные документы, отчеты и т. п.).

Одним из важнейших аспектов проблемы обеспечения безопасности информационных систем являются определение, анализ и классификация возможных угроз безопасности данной информационной системы. Перечень угроз, оценки вероятностей их реализации, модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты информационной системы.

Любая информационная система подвержена значительному числу различных видов угроз безопасности. Под угрозой информационной безопасности передачи данных (в данном случае КИМ и результатов экзамена) при подготовке и проведении экзамена понимается возможное вмешательство заинтересованного лица в информационную сферу процесса. Непредотвращение, необнаружение и неликвидация последствий такого вмешательства может привести к ухудшению заданных качественных характеристик процесса подготовки и проведения экзамена.

Все угрозы информационной безопасности процесса подготовки и проведения экзамена можно поделить на два больших класса: внутренние и внешние. Перечислим все предполагаемые виды внешних и внутренних угроз на разных этапах ЕГЭ (см. табл. 1).

Следует отметить, что внутренняя угроза — это угроза, находящаяся внутри системы или другими словами, это угроза, которую могут спровоцировать действия субъектов самой системы подготовки и проведения ЕГЭ.

На рис. 2 показана схема возможных воздействий злоумышленника на этапах подготовки и проведения экзамена, а также последствия его действий. На рис. 3 представлена схема возможных воздействий злоумышленника на этапе обработки результатов экзамена, а также последствия его действий.

Немаловажно, что каждому из этапов отведен определенный интервал времени, и в связи с этим различного рода нарушения ограничены по времени.

Этап подготовки экзамена. Подготовка к экзамену начинается с создания контрольно-

измерительного материала (КИМ) Федеральным институтом педагогических исследований (ФИПИ). Далее КИМ передается в Центр тестирования, где его тиражируют, формируют пакеты (секьюрпаки — пластиковые, заклеивающиеся пакеты) и пересылают при помощи доверенного лица в ОУО РФ. ОУО РФ, в свою очередь, распределяет эти пакеты между РЦОИ. Одной из задач РЦОИ является распределение и передача КИМ в ППЭ. Каналы передачи КИМ от ФИПИ к РЦОИ будем считать доверительными относитель-

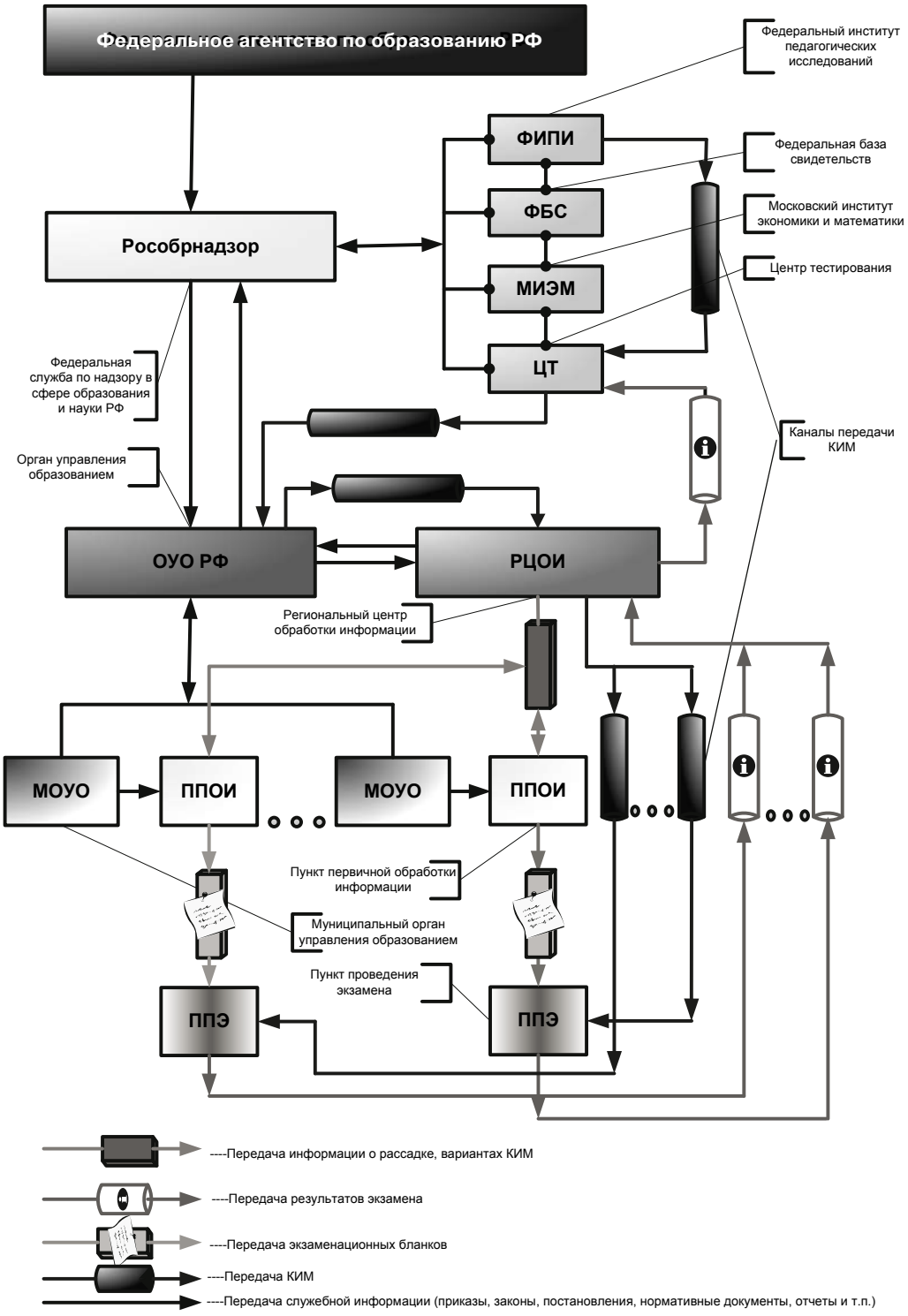


Рис. 1. Информационная модель подготовки и проведения ЕГЭ

Таблица 1

Внешние и внутренние угрозы

Этап подготовки	
Внешняя	*Внутренняя*
НСД к КИМ	Сбой работы программно-аппаратных средств
Подмена КИМ	Сбой энергопитания
Кража КИМ	Саботаж персонала
Сбой энергопитания	
Этап проведения	
Кража пакетов с бланками	Утрата пакетов с бланками
Кража КИМ	Утрата КИМ
Сбой энергопитания	Подмена индивидуальной работы
	Использование шпаргалок
	Использование подсказок
	Сбой энергопитания
	Саботаж персонала
Этап обработки результатов	
Подмена работы в пакете	Подмена индивидуальной работы сотрудниками
Кража бланков с ответами	Утрата бланков с ответами
Перехват файлов с результатами	Изменение результатов персоналом
Сбой работы программно-аппаратных средств	Сбой работы программно-аппаратных средств
Сбой энергопитания	Сбой энергопитания
Сбой работы внешнего канала связи	Сбой работы внешнего канала связи

но каналов передачи от РЦОИ к ППЭ. Гарантировать абсолютную надежность канала от ФИПИ к РЦОИ невозможно. Всегда существует вероятность того, что эта надежность будет нарушена при наложении определенных условий (стихийные бедствия и казусы природы способны повлиять на процесс, но они не зависят от человека). Нельзя отрицать тот факт, что всегда найдется кто-то, преследующий личные цели, кто захочет вмешаться в процесс и что-нибудь «подправить». Первоначально будем рассматривать не цели, которыми мог бы руководствоваться злоумышленник, а действия, которые он может совершить, и результат этих действий.

Согласно американскому стандарту по защите («Оранжевая книга») все вопросы безопасности информации описываются доступами субъектов (людей) к объектам (КИМ, бланки с результатами). Значит, для рассмотрения вопросов безопасности и защиты информации достаточно рассматривать множество объектов и последовательность доступа к ним.

В момент нахождения КИМ в РЦОИ и передачи их в ППЭ возможны следующие виды нарушений: несанкционированный доступ (НСД) к КИМ; подмена КИМ; кража КИМ.

НДС к КИМ — это вскрытие пакета, в котором хранятся варианты заданий. Вскрытие пакета влечет за собой возможность получения копий КИМ и матрицы ответов, ее массовое распространение. Как результат — фальсификация ответов и, соответственно, получение недостоверных результатов о качестве образования. Заметим, что фальсификация может быть как массовой, так и единичной (все зависит от того, насколько «добрым» был злоумышленник, получивший копию КИМ, насколько «щедрым» был тот, кому тоже захотелось «легких» результатов, и как «хорошо» они сумели договориться). Единичную фальсификацию (даже в пределах одного ППЭ) достаточно трудно распознать, а вот массовая достаточно хорошо прослеживается по полученным результатам (ну не могло же абсолютное большинство правильно решить задания, при этом одинаково мысля и делая идентичные ошибки). Ответственность за хранение КИМ возлагается на руководителя РЦОИ (единственный человек, имеющий непосредственный доступ к данным материалам).

Подмена КИМ — срыв процесса экзамена. О том, что КИМ был подменен, станет понятно на этапе обработки при наложении

матрицы ответов на бланки с результатами экзамена. Совершенно понятно, что данная ситуация крайне нежелательна ни для стороны, проводящей экзамен, и тем более не для стороны, сдающей экзамен. Можно предположить, что подмена произойдет, но при этом должно непременно выполниться два условия: доступ к КИМ и наличие «ложного» КИМ. Такое событие также маловероятно, т. к. ведется строгий учет всех экземпляров КИМ за прошлые годы, а доступ к КИМ имеет ограниченное количество людей.

Возможен также вариант кражи КИМ, но это не так существенно, как подмена, т. к. украденный КИМ можно заменить на другой, не прерывая процесс подготовки и проведения экзамена. Вся неприятность данного варианта в том, что человек, ответственный за сохранность КИМ, может утратить репутацию доверенного лица.

Существует также такая угроза, как сбой работы программно-аппаратных средств. Данную угрозу можно минимизировать, используя источники автономного питания для аппаратных средств и производя тестирование программного обеспечения.

Этап проведения экзамена. Этап проведения экзамена — самый непродолжительный по времени по сравнению с остальными этапами, но не менее значимый по своей сути. В момент проведения экзамена возможны

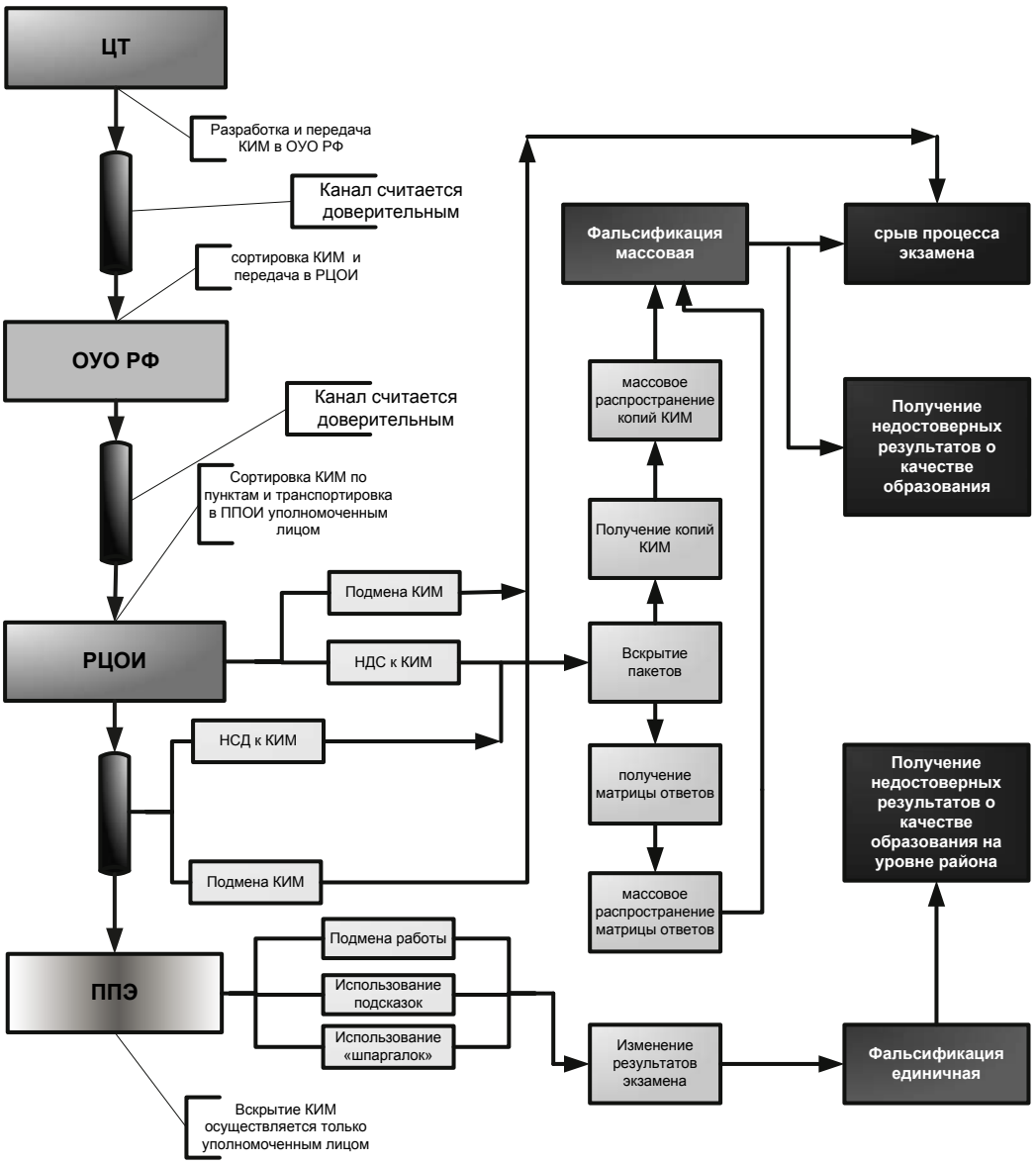


Рис. 2. Схема возможных воздействий злоумышленника на этапах подготовки и проведения экзамена

такие несанкционированные действия: подмена работы (на некоторое время вариант задания передается третьему лицу, которое его решает и передает ответы экзаменуемому лицу); использование «подсказок»; использование «шпаргалок». Все эти действия ведут к фальсификации и «искажению картины качества» образования. Возможна как единичная, так и массовая фальсификация.

Особый интерес для нас представляет первый вариант несанкционированного действия: подмена работы. Графически данное действие с последующими последствиями показано на рис. 4.

Для того чтобы подменить задание, необходимо: знать номер варианта; иметь задание; найти предметника, который решит это задание (не стоит забывать, что время ограничено); сделать ксерокопию бланков ответов; передать результаты. Знать (или узнать) номер варианта могут: Руководитель РЦОИ; Администратор РЦОИ; Оператор ППОИ; Руководитель ППЭ; Организатор в аудитории. Ясно, что каждый из этих людей будет владеть информацией (в данном случае «номером варианта») в разные моменты времени, а соответственно для того, чтобы организовать подмену результатов, у них будет определенное количество времени. Знать (узнать) задание могут: Руководитель РЦОИ; Администратор РЦОИ; Оператор ППОИ; Руководитель ППЭ; Организатор в аудитории. Сделать ксерокопию бланков ответов и передать результаты могут: Руководитель ППЭ; Организатор в аудитории. Можно предположить, что руководитель ППЭ и организатор аудитории договорились, тогда подменить бланк не составит особого труда. Подменить бланк так же можно и в момент доставки результатов экзамена в РЦОИ, все, что для этого нужно — это найти нужный пакет и поменять бланки. Сделать это может руководитель ППЭ, который является ответственным за сбор и доставку бланков.

Этап обработки результатов. Этот этап по времени занимает порядка трех дней. И на этом этапе возможны следующие нарушения: НДС к бланкам экзамена; кража результатов экзамена; изменение результатов экзамена персоналом.

НДС к бланкам экзамена (вскрытие пакета и подмена бланка) ведет к изменению результатов экзамена (банальная фальсификация), и как следствие — неправильная оценка качества образования. Кража бланков с ответами автоматически ведет к срыву экзаменационного процесса и невозможности оценить уровень качества образования. Бланки с ответами имеют ценность до того, как их отсканировали и занесли в электрон-

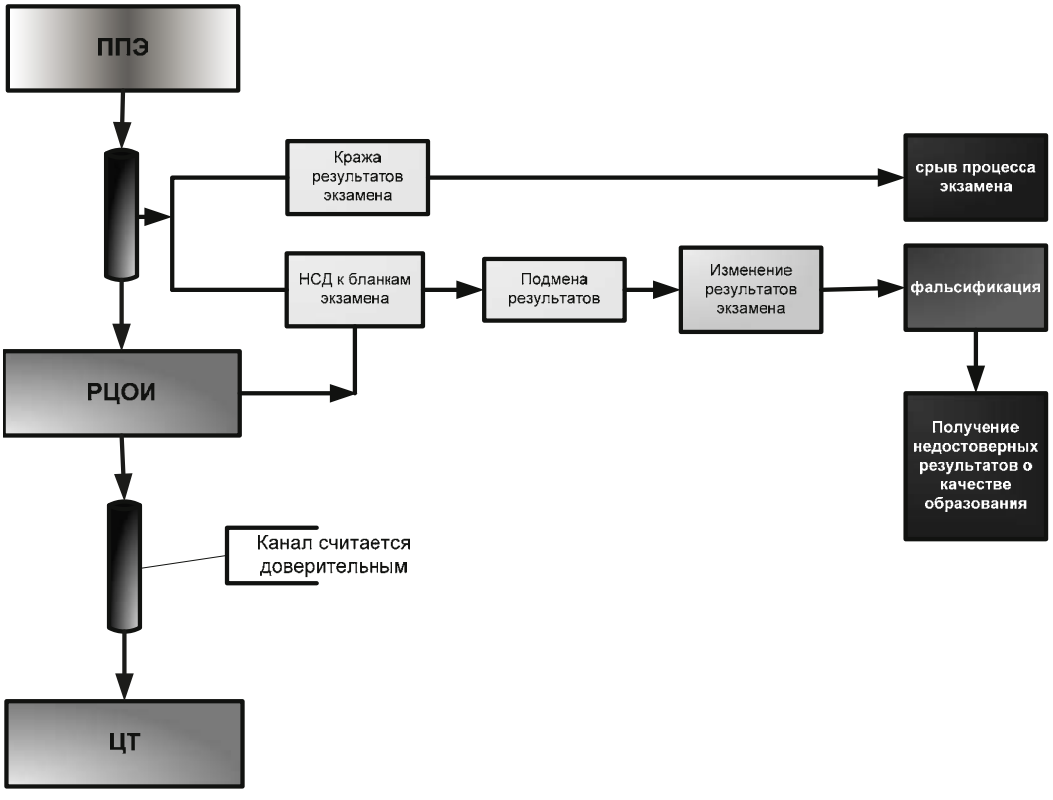


Рис. 3. Схема возможных воздействий злоумышленника на этапе обработки результатов экзамена

ную базу данных, несмотря на то, что эти бланки хранятся еще в течение трех лет. Изменить результаты, представленные в электронном виде, может только администратор РЦОИ. В момент проведения экзамена и обработки результатов локальная сеть РЦОИ отключена от внешней сети.

Все угрозы, связанные с технической стороной работоспособности системы, по возможности пытаются минимизировать.

Угрозы конфиденциальности, целостности и доступности при подготовке и проведении ЕГЭ

Нарушение конфиденциальности на этапах подготовки и проведения экзаменационного процесса есть не что иное, как НДС к информационным ресурсам системы. На этапе подготовки проведения экзаменационного процесса нарушение конфиденциальности заключается в получении доступа к пакетам с КИМ, а следовательно, создание их копии и получение матрицы ответов.

Нарушение целостности на этапе подготовки проведения экзаменационного процесса — уничтожение информации (кража) или ее модификация с целью срыва процесса (подмена КИМ); на этапах проведения и обработки результатов процесса проведения экзаменационного процесса — модификация информации (изменение результатов тестирования с целью «повышения» отметки).

Нарушение доступности на этапе подготовки проведения экзаменационного процесса — ухудшение качественных характеристик процесса (получение и массовое распространение матрицы ответов приводит к получению недостоверных сведений о качестве образования); на этапах проведения экзаменационного процесса — нарушение возможности проведения, срыв экзаменационного процесса (подмена КИМ, кража бланков с результатами).

Следует отметить, что все три вида угроз взаимосвязаны: нарушение конфиденциальности влечет за собой нарушение целостности, а нарушение целостности — нарушение доступности. Нарушение информационной безопасности приводит либо к срыву процесса проведения экзамена, либо к недостоверности результатов экзамена.

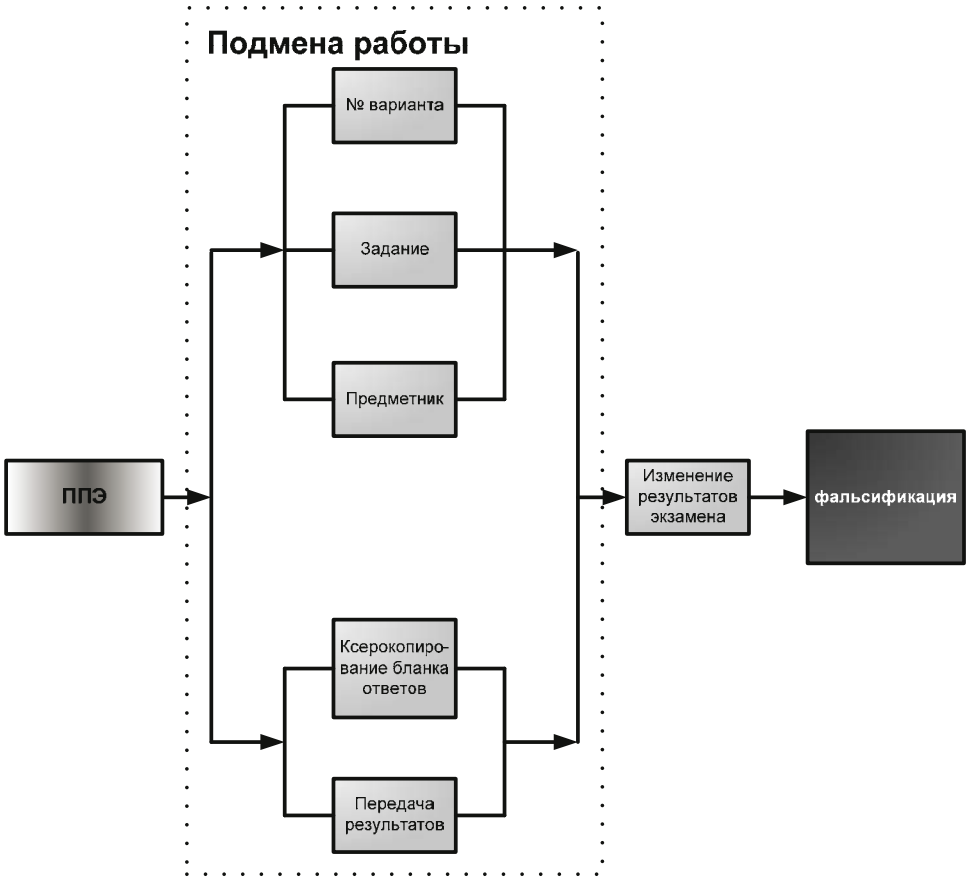


Рис. 4. Подмена работы

На рис. 5 представлена графическая модель нарушений при проведении ЕГЭ.

Ценность информации. Чтобы защитить информацию, надо затратить силы и средства, а для этого надо знать, какие потери мы могли бы понести. Ясно, что в денежном выражении затраты на защиту не должны превышать возможные потери.

Далеко не всегда возможно и нужно давать денежную оценку информации. Например, оценка личной информации, политической информации или военной информации не всегда разумна в денежном исчислении. Однако подход, связанный со сравнением ценности отдельных информационных элементов между собой, по-прежнему имеет смысл. В нашем случае мы тоже можем применить подход, связанный со сравнением ценностей. Только следует заметить, что ценность информации будет меняться со временем. Другими словами, до начала экзамена КИМ будет иметь очень высокую ценность, в момент проведения и тем более после окончания результатов ценность КИМ резко упадет (рис. 6).

Модель нарушителя. В каждом конкретном случае, исходя из конкретной технологии обработки информации, может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной автоматизированной системы.

Известно, что при разработке модели нарушителя определяются: предположения о категориях лиц, к которым может принад-

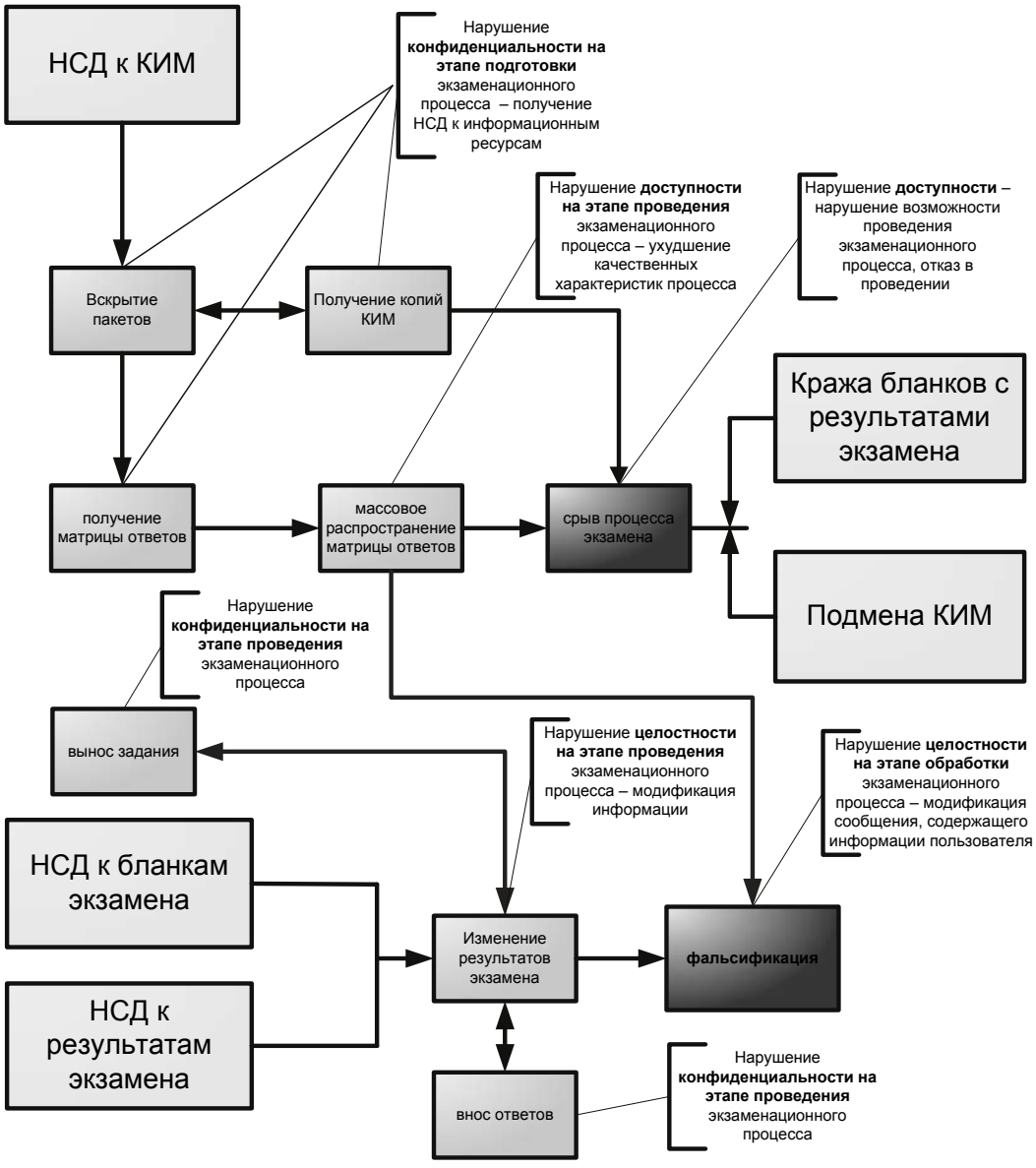


Рис. 5. Графическая модель нарушений при проведении ЕГЭ

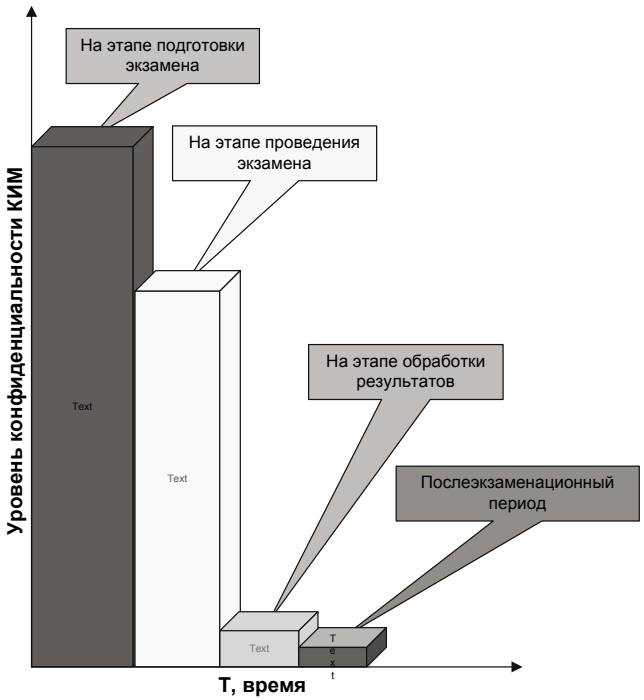


Рис. 6. Зависимость ценности КИМ от времени

лежать нарушитель; предположения о мотивах действий нарушителя (преследуемых нарушителем целях); предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах); ограничения и предположения о характере возможных действий нарушителей.

В системе нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Перечислим возможных внешних и внутренних нарушителей информационной системы процесса подготовки и проведения ЕГЭ (табл. 2).

Таблица 2

Внутренние и внешние нарушители

	Внутренние нарушители
1	*Пользователь средств информационного сопровождения организации и проведения ЕГЭ (персонал)*
	Руководитель РЦОИ
	Администратор РЦОИ
	Операторы РЦОИ
	Вспомогательный персонал РЦОИ
	Ответственный организатор в ППЭ
	Организатор в аудитории соответствующего ППЭ
	Эксперты
2	*Технический персонал, обслуживающий здания*
	Уборщики
	Электрики
	Сантехники
	Сотрудники службы безопасности
	и др. лица, имеющие доступ к помещению, где расположены компоненты информационной системы

	Внешние нарушители
1	*Экзаменуемые*
2	*Представители экзаменуемых лиц*
	Родители
	Представители школ
3	Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энергоснабжение, телефонная связь)
4	Представители конкурирующих организаций (по производству ПО и организации процесса экзамена)
5	Представители общественно-политических организаций
6	Любые лица или группа лиц за пределами контролируемой территории

Нарушителей также можно поделить по категориям заинтересованности (рис. 7).

Обратимся к нашему информационному процессу подготовки и проведения ЕГЭ, а также к тем лицам, которые участвуют в этом процессе. Полномочия и обязанности людей — это их роли в данном процессе. Рассмотрим, какие именно роли выполняют те или иные лица на уровне РЦОИ и ППЭ (табл. 3).

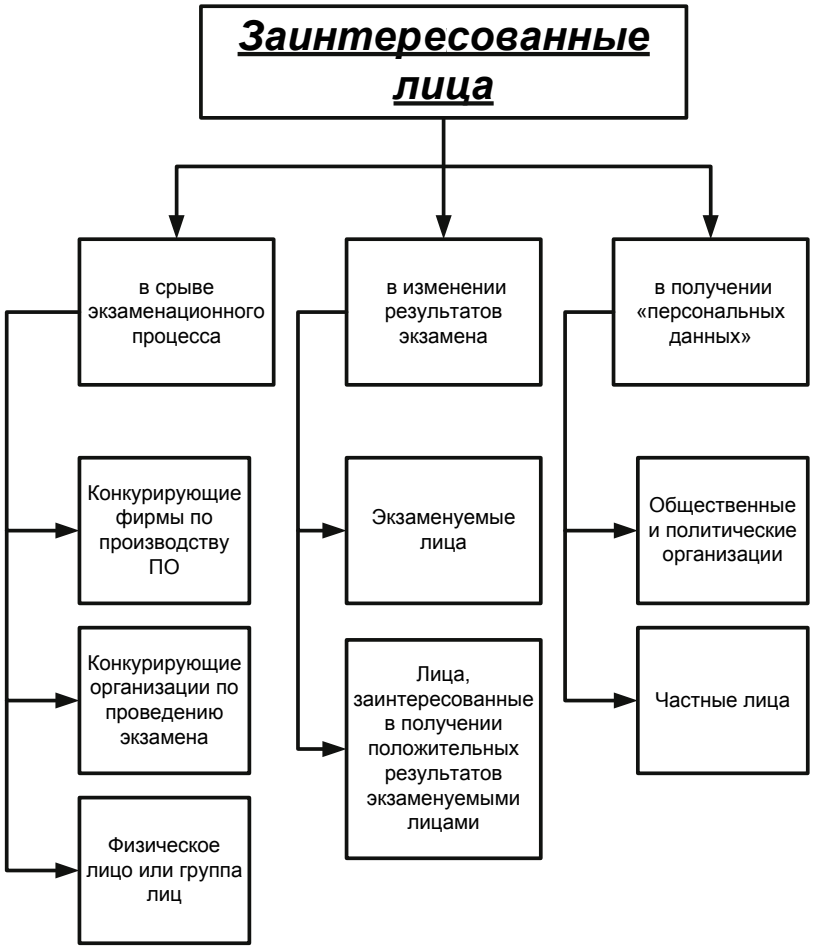


Рис. 7. Классификация нарушителей по заинтересованности

Таблица 3

Должностные лица и их обязанности

Должностное лицо	Обязанности
Руководитель РЦОИ	Обеспечивает секретность упаковки комплектов документов для проведения экзамена, организует жеребьевку ППЭ среди ПЭК и уполномоченных РЦО, по протоколу выдает и принимает у уполномоченных РЦО полные комплекты документов проведения экзамена, в процессе обработки контролирует весь поток бумажных материалов между вычислительным комплексом, экспертами, дежурными и местом хранения. Проверяет правильность введенных ключей. Совместно с уполномоченным РЦО этого ППЭ производит сверку количества привезенных и обработанных бланков по соответствующим протоколам.
Администратор РЦОИ	Устанавливает и настраивает программно-аппаратный комплекс для подготовки, проведения ЕГЭ. Экспорт результатов обработки ответов на задания типа «А», «В» и результатов проверки ответов на задания типа «С» в файл данных установленного формата в ЦТ.
Оператор РЦОИ	Работает за консолью вычислительного комплекса, производит операции сканирования, верификации и печати всех документов. Вводит ключи. Никаких административных функций не выполняет.
Вспомогательный персонал РЦОИ	Носит бланки проверки от вычислительного комплекса к экспертам, раздает их, собирает проверенные и приносит их на обработку.
Эксперты	Провести проверку всех выданных заданий типа «С» на основании инструкции для экспертов по проверке задания «С» и выставить один балл из набора возможных.
Уполномоченный ПЭК	Принимает по протоколу комплект документов у уполномоченного лица, распределение конвертов по аудиториям, выдача дополнительных бланков ответов «С», контроль пересчета бланков ответов после экзамена, заполнение протокола передачи бланков из ППЭ в РЦОИ, оформляет протоколы в случае обнаружения ошибки в регистрационных данных школьника и в случае, если ученик явился на экзамен без удостоверения личности.
Ответственный организатор ППЭ	Перевозка полных комплектов документов проведения экзамена в ППЭ, распределение дежурных по аудиториям, контроль соблюдения регламента проведения экзамена, регистрация нарушений в протоколе, контроль секретности упаковки документов после экзамена и их перевозка в МЦА. Присутствует в процессе обработки бланков своего ППЭ, при необходимости вручную все их пересчитывает.
Ответственный дежурный	Пропускает по ведомости учеников в аудиторию, зачитывает инструкцию школьникам, раздает черновики, следит за порядком, после завершения экзамена формирует итоговую ведомость проведения экзамена по своей аудитории.
Дежурные по аудитории	Помогают ученикам занять свое место, отмечают явку на экзамен, проверяют качество авторучек, раздают именные бланки ответов и КИМ, участвуют в процессе выдачи дополнительного бланка ответов «С», собирают все бланки ответов и КИМ, регистрируют количество выданных и сданных бланков в своей ведомости проведения экзамена.
Дежурный у входа в ППЭ	Открывает на вход ППЭ, по ведомости на основании удостоверения личности пропускает в знание учеников и ответственных от школ, предотвращает проход в ППЭ посторонних лиц.
Дежурный на этаже	Направляет учеников в аудитории, следит за порядком и отсутствием посторонних лиц на территории ППЭ во время проведения экзамена.
Общественные наблюдатели	Информирование общественности о ходе проведения Единого государственного экзамена и осуществление общественного наблюдения за проведением ЕГЭ.

Выше была приведена классификация нарушителей по заинтересованности. Следует отметить, что на первый план все же выходит «заинтересованность в подмене результатов (их улучшении)».

Приведем таблицу, в которой покажем, кто заинтересован, какой вид фальсификации (локальная или массовая) может произойти, какие люди и с каким уровнем возможностей могут содействовать в «изменении» результатов (табл. 4).

Таблица 4

Заинтересованные лица и их уровни возможностей

Заинтересованное лицо	**Вид фальс.**	**Кто может содействовать**	**Уровень возможностей**
1	2	3	4
экзаменуемые	локальная	Организатор ППЭ	средний
		Другие учащиеся	низкий
родители экзаменуемых	локальная	Руководитель РЦОИ	высокий
		Администратор РЦОИ	высокий
		Операторы РЦОИ	средний
		Вспомогательный персонал РЦОИ	низкий
		Ответственный организатор в ППЭ	средний
		Организатор в аудитории соответствующего ППЭ	низкий
		Технический персонал, обслуживающий здания	низкий
		Эксперты	низкий
		Дежурный у входа в ППЭ	низкий
		Дежурный на этаже	низкий
		Ответственный дежурный	низкий
сотрудники ОУ (директор школы)	массовая	Руководитель РЦОИ	высокий
		Администратор РЦОИ	высокий
		Операторы РЦОИ	средний
		Вспомогательный персонал РЦОИ	низкий
		Ответственный организатор в ППЭ	средний
		Организатор в аудитории соответствующего ППЭ	низкий
		Технический персонал, обслуживающий здания	низкий
		Эксперты	низкий
		Ответственный дежурный	низкий
		Ответственный дежурный	низкий
		Ответственный дежурный	низкий
сотрудники МОУО	массовая	Руководитель РЦОИ	высокий
		Администратор РЦОИ	высокий
		Операторы РЦОИ	средний
		Вспомогательный персонал РЦОИ	низкий
		Ответственный организатор в ППЭ	средний
		Организатор в аудитории соответствующего ППЭ	низкий
		Технический персонал, обслуживающий здания	низкий
		Эксперты	низкий

Окончание табл. 4

1	2	3	4
		Ответственный дежурный	низкий
		Ответственный дежурный	низкий
репетиторы	локальная	Руководитель РЦОИ	высокий
		Администратор РЦОИ	высокий
		Операторы РЦОИ	средний
		Вспомогательный персонал РЦОИ	низкий
		Ответственный организатор в ППЭ	средний
		Организатор в аудитории соответствующего ППЭ	низкий
		Технический персонал, обслуживающий здания	низкий
		Эксперты	низкий
		Ответственный дежурный	низкий
		Ответственный дежурный	низкий
		Ответственный дежурный	низкий

Из таблицы видно, что сами по себе люди с низким и средним уровнем возможностей не способны произвести фальсификацию результата. Но вот в сговоре это вполне возможно.

Как уже раньше было сказано, процесс подготовки и проведения экзамена имеет временную зависимость (рис. 8). И на каждом этапе характерное лицо (или группа лиц) может неким образом повлиять на результаты экзамена (способствовать фальсификации).

На рис. 8 представлены лица и группы лиц, которые, используя свое служебное положение, могут повлиять на результаты экзамена.

Рассмотрим эмпирическое предположение.

Пусть существует некоторое число «желающих» изменить результаты экзамена.

Для большей наглядности введем ориентировочную шкалу вероятности события (угрозы) «удачного изменения результатов» (вероятность удачи):

P = 0,001 — событие практически не возможно;

P = 0,01 — событие маловероятно;

P = 0,05 — событие возможно;

P = 0,2 — событие вполне возможно.

Опираясь на это, определим, сколько в среднем работ может быть фальсифицировано в одном ППЭ и по региону в целом.

1. Возможность фальсификации практически невозможна (p = 0,001).

За один раз в ППЭ сдает экзамен порядка 150 человек. Тогда в среднем будет фальсифицировано

$$M = p \cdot n = 0.001 \cdot 150 = 0.15 \text{ работ,} \quad (1)$$

или 0,1 % от общего числа.

Используя Биноминальную формулу

$$p(m) = C_n^m p^m (1-p)^{n-m} = \frac{n!}{m! \cdot (n-m)!} p^m (1-p)^{n-m} \quad (2)$$

определим вероятность подмены одной и более работ. Результаты приведены в табл. 5.

Таблица 5

Вероятность фальсификации m работ

Количество фальсифицированных работ	**Значение вероятности p(m)**
0	0,861
1	0,129
2	$9{,}637e^{-3}$
3	$4{,}759e^{-4}$
4	$1{,}751e^{-5}$
5	$5{,}117e^{-7}$
6	$1{,}238e^{-8}$
7	$2{,}549e^{-10}$
8	$4{,}561e^{-12}$
9	$7{,}203e^{-14}$
10	$1{,}017e^{-15}$
11	0
12	0

Из таблицы видно, что вероятность фальсификации даже одной работы очень мала.

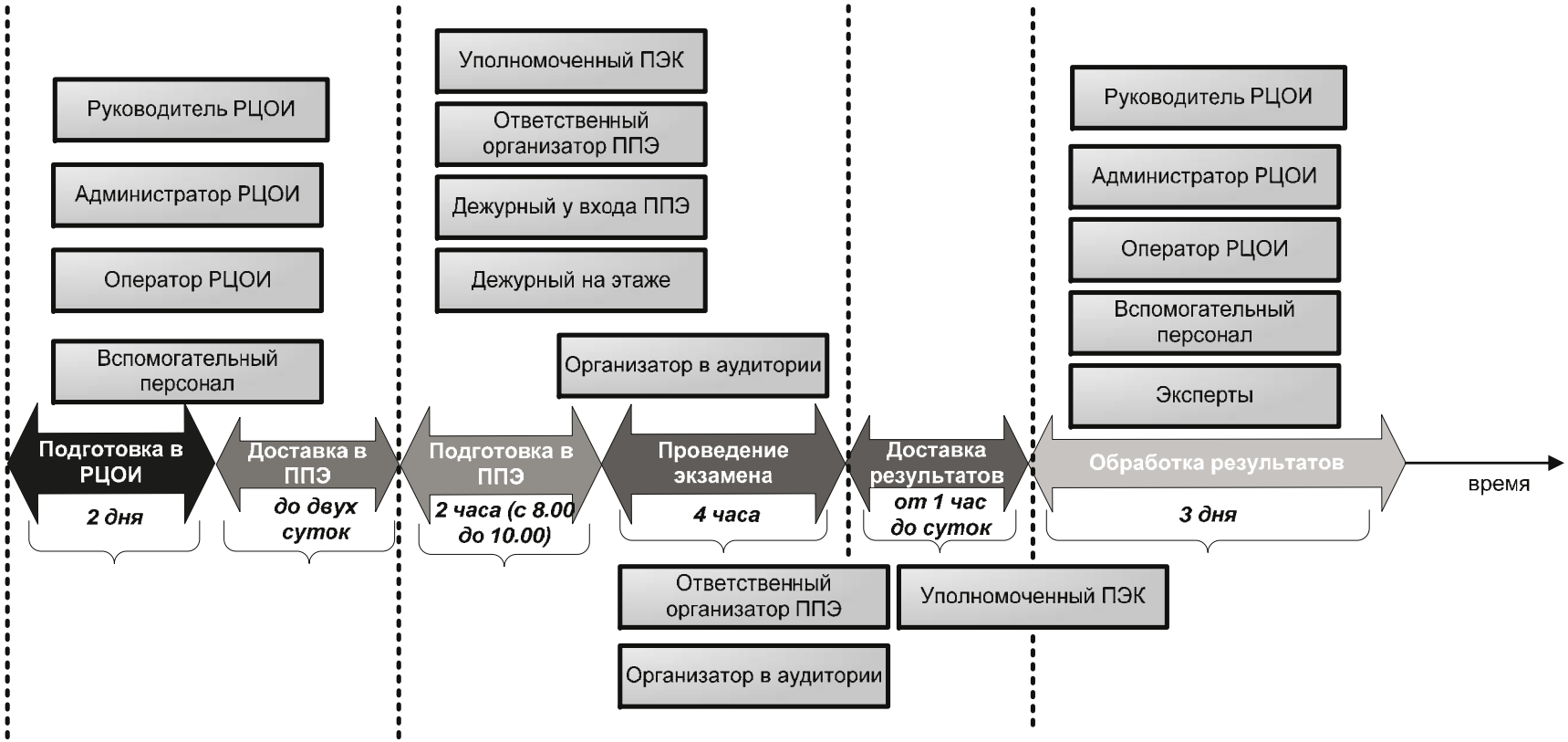


Рис. 8. Временной интервал процесса подготовки и проведения экзамена и люди, которые могут повлиять на результаты экзамена

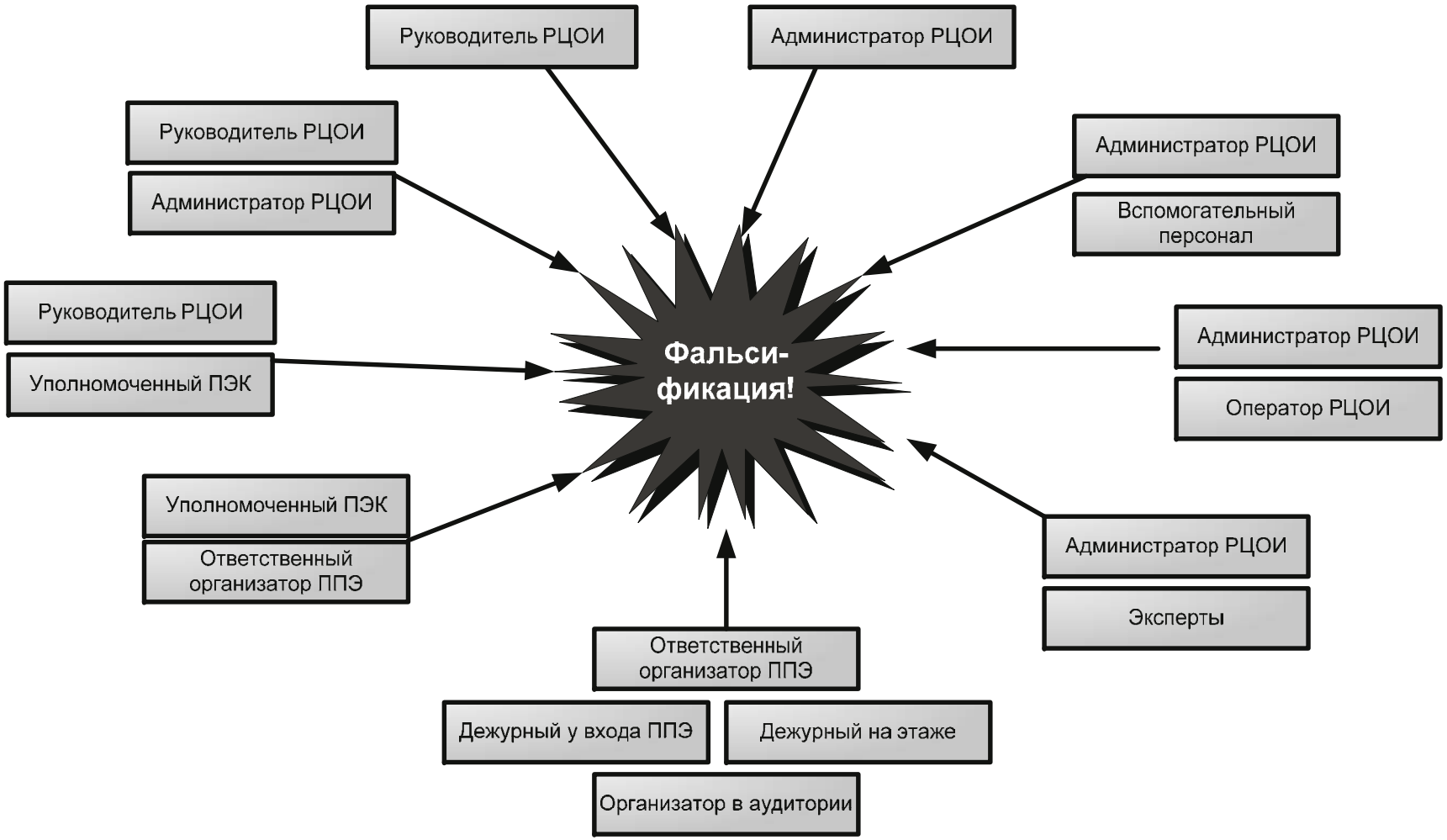


Рис. 9. Группы лиц, которые способны сфальсифицировать данные

2. Фальсификация маловероятна (p = 0,01).

Воспользуемся формулами 1 и 2:

$M = 0.01 \cdot 150 = 1.5$ работ, или 1 % от общего числа.

Таблица 6

Вероятность фальсификации m работ

Количество фальсифицированных работ	Значение вероятности p(m)
0	0,221
1	0,336
2	0,252
3	0,126
4	0,047
5	0,014
6	$3{,}363e^{-3}$
7	$6{,}988e^{-4}$
8	$1{,}262e^{-4}$
9	$2{,}011e^{-5}$
10	$2{,}864e^{-6}$
11	$3{,}682e^{-7}$
12	$4{,}308e^{-8}$

По сравнению с предыдущим пунктом вероятность фальсификации одной работы возросла в 2,6 раза.

3. Событие подмены работы вполне возможно (p = 0,05).

Снова воспользуемся формулами 1 и 2:

$M = 0.05 \cdot 150 = 7.5$ работ или 5 % от общего числа.

Таблица 7

Вероятность фальсификации m работ

Количество фальсифицированных работ	Значение вероятности p(m)
0	$4{,}556e^{-4}$
1	$3{,}596e^{-3}$
2	0,014
3	0,037
4	0,071
5	0,109
6	0,138
7	0,15
8	0,141
9	0,117
10	0,087
11	0,058
12	0,035

4. Событие фальсификации вполне возможно (p = 0,2).

$M = 0.2 \cdot 150 = 30$ работ, или 20 % от общего числа

$$p(30) = 0.081.$$

Получается, что при таком условии фальсификация 30 работ — вполне вероятное событие.

Из всех полученных расчетов следует, что результаты Единого государственного экзамена можно считать достоверными, если созданы такие условия, при которых количество фальсифицированных работ может составлять менее 0,1 % от общего числа.

Таким образом, в результате создания информационной модели процесса подготовки и проведения ЕГЭ и анализа угроз этому процессу было выявлено, что наиболее вероятными являются те угрозы, которые ведут к фальсификации данных. При анализе прав доступа и обязанностей лиц, задействованных в подготовке и проведении ЕГЭ, были выделены лица и группы лиц, уровень возможностей которых достаточен для фальсификации результатов. Путем расчетов было получено количество фальсифицированных работ, необходимое для того, чтобы результаты Единого государственного экзамена можно было считать достоверными.

ЦАРЕВ Евгений, заместитель директора департамента продуктов и услуг компания Leta.

TSAREV Eugene, deputy director of products and services company Leta.

ЛЯШЕНКО Екатерина, «Укртелеком».

LIASHENKO Catherine, «Ukrtelecom»

УДК 004.032.26 + 004.52
ББК Ч231.3

В. С. Ковалев, Т. Ю. Зырянова

Экспертное оценивание в управлении информационной безопасностью

V. S. Kovalev, T. Yu. Zyryanova

Expert assessment in information security management

Статья посвящена проблемам управления информационной безопасностью. В частности, затронуты вопросы оценки уровня информационного риска, а также выбора эффективных мер по защите информации. В качестве решения подробно рассматриваются различные методы экспертного оценивания, хорошо зарекомендовавшие себя в области управления.

***Ключевые слова**: информационная безопасность, угрозы безопасности, экспертное оценивание, уровень риска.*

In particular, it deals with the issues of assessing the level of information security risks and selection of efficient information protection measures. A detailed description is given of certain expert assessment methods that have proved to be efficient in the area of information security management and that may be offered as possible solutions.

***Keywords**: Information security, security threats, expert assessment, risk level.*

Введение

Управление любой организацией связано с принятием бесчисленного множества решений, при этом даже незначительное на первый взгляд решение может серьезно повлиять на функционирование организации в целом. Именно поэтому каждое решение должно подвергаться анализу, а выбор из множества альтернативных решении должен быть обоснованным. Также очевидно, что любая организация функционирует во внешней враждебной среде. Информация, как неотъемлемая часть бизнеса, подвергается непрерывным воздействиям со стороны внешней среды и требует адекватной защиты от этих воздействий. Целью данной статьи является описание того, каким образом можно оценить потенциал каждой угрозы безопасности информационных ресурсов и как выбрать наиболее эффективные меры борьбы с этими угрозами.

Для того чтобы определить уровень риска, связанный с той или иной угрозой информационной безопасности, существует множество методов, однако большая часть из них основана на экспертных оценках. Экспертные оценки — это суждения высококвалифицированных специалистов-профессионалов, высказанные в виде содержательной, качественной или количественной оценки объекта, предназначенные для использования при принятии решений[1]. Собрав мнения экспертов — специалистов информационной безопасности, можно использовать их в качестве входных данных для математического моделирования, т. о. достигая наиболее объективной и точной оценки уровня информационного риска.

Применение методов экспертного оценивания для определения уровня информационного риска наиболее целесообразно, прежде всего, потому, что информационные ресурсы находятся в неопределенной, трудно формализуемой среде, на которую может влиять множество случайных факторов. Также не существует надежной теоретической основы, которая бы позволила оценить информационный риск без участия экспертов, например на основе статистики.

1. Общие сведения об экспертном оценивании

Основной задачей экспертного оценивания в области информационной безопасности является определение ценности информационного ресурса (актива), а также вероятности реализации угрозы с учетом существующих уязвимостей, модели предполагаемого нарушителя и принятых мер защиты. Кроме того, экспертное оценивание может использоваться для определения наиболее эффективных контрмер. Оценка,

выдаваемая экспертами, может быть как качественной, так и количественной.

Для принятия решений эксперты должны обладать полной информацией о проблеме, поэтому экспертному оцениванию предшествует комплексное обследование объекта защиты и среды, в которой он функционирует. Обследование подразумевает сбор информации о структуре информационной системы, информационных связях, механизме обработки информации, компетенции обслуживающего персонала, документационном обеспечении, физической охране и т. д.

Экспертиза состоит из ряда этапов, которые представлены на рис. 1.

Рис. 1. Основные этапы экспертного оценивания

Всякое экспертное оценивание начинается с создания рабочей группы во главе с руководителем. В задачи руководителя входят организация и проведение экспертного исследования в целом, а также анализ мнений экспертов и формулировка заключения по результатам исследования. В зависимости от масштабов исследования в рабочую группу могут входить аналитики, операторы автоматизированных систем, специалисты по работе с экспертами (интервьюеры) и т. д. На рабочей группе лежит ответственность за формирование компетентной экспертной комиссии, за ее принципиальную способность решить поставленную задачу.

Очевидно, что для принятия обоснованных решений большое значение имеют род занятий и стаж работы эксперта по профилю оцениваемого объекта. При необходимости учитывается уровень и характер образования, опыт научной деятельности, публикации и т. д. Число экспертов зависит от требуемой точности оценок, допустимой трудоемкости оценочных процедур.

Важным этапом экспертного оценивания является разработка подробного плана или сценария. Необходимо определиться, в какой форме будет проходить экспертное оценивание — интервьюирование или анкетирование, а также выбрать методы анализа полученных данных. Следует четко представлять, какие именно данные необходимо получить от экспертов, и в какой форме должны быть представлены эти данные для проведения последующего анализа.

Существует масса методов получения экспертных оценок. В одних с каждым экспертом работают отдельно, при этом эксперт не знает, кто еще входит в состав экспертной комиссии, а потому высказывает свое мнение независимо от авторитетов и отдельных коллег. В других экспертов собирают вместе для обсуждения проблемы друг с другом, при этом принимают или отвергают аргументы и неверные или недостаточно обоснованные мнения отбрасываются.

Информация, полученная от экспертов, в дальнейшем подлежит анализу с применением различных формально-математических методов. Т. к. мнения некоторых экспертов могут сильно отличаться от большинства, то итоговый результат может быть вычислен с ошибкой и не соответствовать действительности. Чтобы этого избежать, необходимо заранее выбрать допустимый уровень расхождения мнений экспертов и в дальнейшем при проведении экспертизы ориентироваться на этот уровень.

Далее в статье будут рассмотрены три основных метода экспертного оценивания, которые хорошо себя зарекомендовали в области управления организацией.

2. Методы экспертного оценивания

2.1. Метод Дельфи

Метод Дельфи — инструмент, позволяющий учесть независимое мнение всех участников группы экспертов по обсуждаемому вопросу путем последовательного объединения идей, выводов и предложений и прийти к согласию[2]. Метод основан на анонимных опросах экспертов, т. о. исключаются открытые столкновения между сторонниками противоположенных позиций и влияние мнения большинства. Кроме того, опрос можно проводить экстерриториально, не собирая экспертов в одном месте.

Анализ с помощью метода Дельфи проводится в несколько туров, после каждого тура результаты обрабатываются статистически-

ми методами. На первом туре производится сбор мнений экспертов по заданной проблеме. После первого тура опросов участники экспертной комиссии получают все ответы, данные другими участниками, чтобы уточнить и скорректировать свои позиции.

Например, оценивая угрозу осуществления атаки, приводящей к отказу в обслуживании (DOS-атаки) информационной системы, эксперт ознакомившись с исходными данными, определяет вероятность такой атаки 0,5. В следующем туре, ознакомившись с мнениями других участников опроса, эксперт может прийти к выводу, что он упустил некоторые факторы, влияющие на информационную безопасность, и как следствие, поменять свою оценку. В последующих турах ответы экспертов будут носить все более устойчивый характер и, в конце концов, перестанут изменяться, что является основанием для прекращения опросов. Практика показывает, что для получения устойчивой оценки достаточно четырех туров опроса.

2.2. Метод сценариев

Метод сценариев — это метод декомпозиции задачи прогнозирования, предусматривающий выделение набора отдельных вариантов развития событий (сценариев), в совокупности охватывающих все возможные варианты развития[3].

Метод сценариев дает возможность оценить наиболее вероятный ход развития событий и возможные последствия принимаемых решений. Разрабатываемые экспертами сценарии развития анализируемой ситуации позволяют с тем или иным уровнем достоверности определить возможные тенденции развития, взаимосвязи между действующими факторами, сформировать картину возможных состояний, к которым может прийти ситуация под влиянием тех или иных воздействий. Следует отметить, что каждый отдельный сценарий должен допускать возможность достаточно точного прогнозирования, а общее число сценариев должно быть обозримо.

Составив сценарии реализации угроз информационной безопасности с учетом модели нарушителя, можно выявить наиболее опасные угрозы в зависимости от последствий, к которым они могут привести.

Например, оценивая уровень риска несанкционированного доступа, реализуемого с использованием протоколов межсетевого взаимодействия, необходимо составить детальный каталог сценариев атак и несанкционированных действий, связанных с работой информационной системы в вычислительной сети. Каждый из таких сценариев описывает атаку своего типа, со своим индивидуальным происхождением, развитием, последствиями, возможностями предупреждения. В табл. 1 показан пример такого сценария.

Таблица 1

Пример сценария реализации угрозы

Наименование угрозы	**Атака типа «Отказ в обслуживании»**
1	2
Источник угрозы	Внешний нарушитель
Мотивы нарушителя	Хулиганство, шантаж
Информация, которая может быть доступна нарушителю	Назначение и общие характеристики информационной системы, открытые порты, версии используемых операционных систем и прикладного ПО, данные об уязвимостях операционных систем и прикладного ПО, запущенные службы, методы и способы проведения сетевых атак
Средства реализации угрозы, которые могут быть доступны нарушителю	Доступные в свободной продаже технические средства и ПО, специально разработанные технические средства и ПО
Существующие уязвимости информационной системы, которые могут быть эксплуатированы нарушителем	Отсутствуют сертифицированные по требованиям безопасности средства защиты информации, не осуществляется фильтрация служебных протоколов, не осуществляется обновление операционных систем и прикладного ПО, отсутствует механизм надежной аутентификации технических средств и пользователей информационной системы
Существующие препятствия реализации угрозы	На границе внутренней сети предприятия и внешней сети установлен маршрутизатор с функцией межсетевого экранирования, осуществляется периодическое резервное копирование информации

Окончание табл. 1

1	2
Вероятная продолжительность реализации угрозы	Не более суток
Последствия реализации угрозы	Нарушение доступности информации
Вероятность успешной реализации угрозы	0,6

Сценарий реализации угрозы позволяет определить какая именно характеристика защищаемого объекта будет нарушена: конфиденциальность, доступность, целостность и т. д., тем самым повышается точность оценки ущерба.

Процесс составления сценариев только частично формализуем. Существенная часть рассуждений проводится на качественном уровне, т. к. излишняя формализация и математизация приводит к искусственному внесению определенности там, где ее не существует, либо к использованию громоздкого математического аппарата.

2.3. Метод мозгового штурма

«Мозговой штурм» — оперативный метод решения проблемы на основе стимулирования творческой активности[4].

Данный метод эффективен, прежде всего, в тех случаях, когда требуется найти нестандартное решение. Зачастую при определении необходимых мер по снижению уровня информационного риска ограничиваются самым простым решением — установкой технических средств защиты. Однако это не всегда является оптимальным решением. Метод мозгового штурма позволит найти менее затратные и более эффективные меры, так может быть найдено решение, вообще исключающее какие либо средства защиты.

Метод мозгового штурма представляет собой двухэтапную процедуру решения задачи: на первом этапе генерируются идеи, а на втором — анализируются и развиваются. Таким образом, функции «автора» и «критика» реализуют разные группы участников и в разное время.

В группу генерации идей следует включать представителей всех подразделений организации, от которых так или иначе зависит уровень информационной безопасности — системные администраторы, администраторы безопасности, программисты и т. д.

На этапе генерации идей необходимо строгое соблюдение участниками ряда правил[5]:

● Исключение любой критики: на стадии генерации идей высказывание любой критики в адрес авторов идей (как своих, так и чужих) не допускается. Работающие в группах должны быть свободны от опасений, что их будут оценивать по предлагаемым ими идеям.

● Свободный полет фантазии: эксперты должны попытаться максимально раскрепостить свое воображение. Разрешается высказывание любых, даже самых абсурдных или фантастических идей.

● Идей должно быть много: каждый эксперт должен представить максимально возможное количество идей.

● Комбинирование и совершенствование предложенных идей: эксперты могут развивать идеи, предложенные другими, например, комбинируя элементы двух или трех предложенных идей.

После сбора исчерпывающего количество идей начинается второй, не менее важный этап экспертного оценивания — анализ идей. Анализ результатов осуществляется в следующей последовательности:

1. Удаление повторяющихся, не относящихся к теме или проблеме идей.

2. Расстановка приоритетов (в соответствии с теми критериями, которые для нас наиболее значимы при решении данной задачи). Критерии могут быть такие: скорость, время, деньги, удобство и т. д.

3. Тщательная проработка предпочитаемых идей решения проблемы (что и как необходимо сделать, кто за что отвечает, необходимые сроки, ресурсы, этапы и т. д.).

Следует отметить, что выбор мероприятий по повышению уровня информационной безопасности методом мозгового штурма требует значительных временны́х затрат, главным образом на всесторонний анализ собранных идей.

3. Обработка результатов

Можно выделить несколько наиболее часто применяемых способов обработки экспертных оценок: вычисление среднего арифметического значения, метод большинства, медиана Кемени. Ниже в качестве примера будут рассмотрены варианты обработки результатов экспертного оценивания раз-

личными способами. Оценке подвергается вероятность реализации угрозы информационной безопасности.

Смысл прямой оценки состоит в том, что эксперты определяют для каждой из анализируемых угроз вероятность реализации в интервале [0; 1] (табл. 2).

Таблица 2

Данные экспертизы для определения вероятности с помощью среднего арифметического значения

	Угроза 1	**Угроза 2**	**Угроза …**	**Угроза *j***
Эксперт 1	p_{11}	p_{12}	…	p_{1j}
Эксперт 2	p_{21}	p_{21}	…	p_{2j}
Эксперт…	…	…	…	…
Эксперт *i*	p_{j1}	p_{j2}	…	p_{ij}

Далее вычисляется среднее арифметическое, которое и будет являться итоговым значение вероятности:

$$| P_j |= \frac{\sum_{i=1}^{n} p_{ij}}{n},$$

где P_j — итоговое значение вероятности реализации j-й угрозы ($j = 1, 2, \dots, k$);

p_{ij} — вероятность реализации j-й угрозы, присвоенная i-м экспертом ($i = 1, 2, \dots, n$);

n — количество экспертов.

Медиана Кемени (расстояние Кемени) — это некая мера, позволяющая оценить степень совпадения мнений экспертов. Чем больше мнение одного эксперта отличается от мнений всех остальных экспертов, тем больше расстояние Кемени. Верным будет являться то мнение, которое будет иметь наименьшее расстояние Кемени[6]. Для примера рассмотрим матрицу мнений экспертов, представленную в табл. 3. Элементы матрицы представляют собой вероятности реализации той или иной угрозы информационной безопасности.

Таблица 3

Данные экспертизы для определения вероятности с помощью среднего арифметического значения

	Угроза 1	**Угроза 2**	**Угроза 3**	**Угроза 4**
Эксперт 1	a_1	a_2	a_3	a_4
Эксперт 2	b_1	b_2	b_3	b_4
Эксперт 3	c_1	c_2	c_3	c_4
Эксперт 4	d_1	d_2	d_3	d_4

Далее необходимо вычислить расстояние между мнениями каждой пары экспертов, которое равно сумме модулей разностей элементов, стоящих в одних и тех же столбцах матрицы:

$$r_{ij} = \sum_{k=1}^{n} | a_k - b_k |,$$

где i, j — порядковые номера экспертов ($i = 1…N, j = 1…N$);

k — порядковый номер угрозы ($k = 1…n$).

Т. о. формируется матрица из расстояний r, представленная в табл. 4.

Таблица 4

Матрица векторных расстояний между мнениями экспертов

	Эксперт 1	**Эксперт 2**	**Эксперт 3**	**Эксперт 4**
Эксперт 1	r_{11}	r_{12}	r_{13}	r_{14}
Эксперт 2	r_{21}	r_{22}	r_{23}	r_{24}
Эксперт 3	r_{31}	r_{32}	r_{33}	r_{34}
Эксперт 4	r_{41}	r_{42}	r_{43}	r_{44}

Медиана Кемени (R) представляет собой сумму расстояний между мнениями r:

$$R_i = \sum_{j=1}^{N} r_{i,j}.$$

Совокупное мнение экспертов можно определить как решение оптимизационной задачи:

$$R \to \min.$$

Т. о., итоговое мнение группы представляет собой мнение эксперта, сумма расстояний от которого до всех ответов экспертов минимальна.

Метод большинства основан на том принципе, что практически надежным является мнение, выраженное большинством после подсчета мнений более или менее значительного числа лиц. В табл. 5 представлен пример результатов экспертного оценивания с последующим выводом по методу большинства.

Таблица 5

Данные экспертизы для определения вероятности с помощью метода большинства

	Угроза 1	Угроза 2	Угроза…
Эксперт 1	0,1	0,9	…
Эксперт 2	0,2	0,8	…
Эксперт 3	0,1	1	…
Эксперт 4	0,3	0,9	…

Согласно табл. 5 итоговое значение уровня информационного риска для угрозы 1 будет равно 0,1, для угрозы 2 — 0,9.

4 Установление степени согласованности мнений экспертов

Как уже говорилось ранее, в случае участия в опросе нескольких экспертов расхождения в их оценках неизбежны, и величина этого расхождения имеет важное значение. Групповая оценка может считаться достаточно надежной только при условии хорошей согласованности ответов отдельных специалистов.

Для анализа разброса и согласованности оценок применяются статистические характеристики — меры разброса[7], которые вычисляются разными способами.

Вариационный размах (C):

$$C = x_{max} - x_{min},$$

где x_{max} — максимальная оценка объекта;
x_{min} — минимальная оценка объекта.

Среднее квадратическое отклонение (δ), вычисляемое по формуле:

$$\delta = \sqrt{\frac{\sum_{i=1}^{n}\left(x_i - \overline{x_{ср.}}\right)^2}{n-1}},$$

где x_i — оценка, данная i-м экспертом;
$x_{ср.}$ — среднее значение оценки.

Коэффициент вариации (V), который обычно выражается в процентах:

$$V = \frac{\delta}{x_{ср.}} \cdot 100\%.$$

Заключение

За последнее время методы экспертного оценивания получили существенное развитие и нашли свое применение в самых различных областях. В области информационной безопасности применимы многие технологии, которые уже зарекомендовали себя в менеджменте как наиболее эффективные. Экспертное оценивание является именно такой технологией.

Заранее неизвестно, как поведет себя злоумышленник, и какие средства он может использовать, поэтому невозможно дать стопроцентно точную оценку уровня информационного риска, однако с помощью представленных выше методов экспертного и последующего формального анализа можно добиться значительной точности в определении уровня риска и выбрать наиболее эффективные меры уменьшения этого уровня до приемлемого.

Примечания

[1] *Литвак Б. Г.* Экспертные оценки и принятие решений. — М. : Патент, 1996. — С. 10.
[2] *Малин А. С., Мухин В. И.* Исследование систем управления : учебник для вузов. — М., 2002.
[3] *Орлов А. И.* Менеджмент : учебник. — М. : Изумруд, 2003. — С. 4.
[4] Управление персоналом : словарь-справочник (Электронный ресурс) // http://psyfactor.org/personal/personal12-03.htm (дата обращения: 01.08.2011).
[5] *Гулидова Г. В.* Технология проведения мозгового штурма (Электронный ресурс) // http://www.ct-v.ru/statji_mozgovoy_shturm.htm (дата обращения: 10.08.2011).
[6] *Глухов А. И., Погодаев А. К.* Медиана Кемени в определении приоритетов развития предприятий // Управление большими системами. — Воронеж : ВГАСУ, 2006. — № 14. — С. 40—45.
[7] *Терентьев С. В.* Экономико-математические методы : курс лекций — Орел : ОрелГТУ, 2010.

КОВАЛЕВ Виктор Сергеевич, ассистент кафедры «Системы и технологии защиты информации», Уральский государственный университет путей сообщения.
E-mail: vkovalev@gammaural.ru

KOVALEV Viktor Sergeevich, Assistant of the Chair "Systems and Technologies of Information Protection", Urals State University of Railway Transport (USURT)/
E-mail: vkovalev@gammaural.ru

ЗЫРЯНОВА Т. Ю., канд. техн. наук, доцент кафедры «Системы и технологии защиты информации», Уральский государственный университет путей сообщения.

Zyryanova T. Yu., Candidate of Technical Sciences, Associate Professor of the Chair "Systems and Technologies of Information Protection", Urals State University of Railway Transport (USURT)

УДК 316.777 + 005.72
ББК Ч231.3:Ю941.2

Л. В. Астахова

Информационно-психологическая безопасность в регионе: культурологический аспект

L. V. Astakhova

Information and psychological security in the region: culturological aspect

В статье на основе деятельностного подхода к понятиям «культура», «информационная безопасность» и»информационно-психологическая безопасность» определены понятия «культура информационной безопасности» и «культура информационно-психологической безопасности»; изложены результаты проведенного кафедрой «Информационная безопасность» ЮУрГУ социологического исследования уровня информационно-психологической безопасности жителей города Челябинска; обоснована необходимость системного подхода к формированию культуры информационно-психологической безопасности в УрФО на основе разработки и принятия региональной целевой программы.

***Ключевые слова**: информационно-психологическая безопасность, информационная безопасность, культура, культура безопасности, информационное взаимодействие.*

Based on the activity approach to such concepts as "culture', "information security" and "information and psychological security", the author defines such notions as "culture of information security" and "culture of information and psychological security". The paper also provides the results of the research conducted by the Chair of Information Security of South Ural State University in order to define the level of information and psychological security of the residents of Chelyabinsk. Further, the paper substantiates the necessity to create the culture of information and psychological security in the Urals Federal District by developing and accepting a special region-level program.

***Keywords**: information and psychological security, information security, culture, security culture, information interoperability*

Право человека на благоприятную окружающую среду, достоверную информацию о ее состоянии закреплено в 42-й статье Конституции РФ и Федеральном законе об охране окружающей среды. Указанный закон утвердил право граждан на охрану здоровья от неблагоприятного воздействия окружающей среды, вызванного хозяйственной или *иной* деятельностью. Помимо природной среды обитания человека объективно существует информационная среда его обитания, роль и значение которой стремительно возрастает по мере дальнейшего становления информационной цивилизации. Эта среда оказывает на человека активное влияние. Она влияет на формирование и функционирование его личности, на его духовное, интеллектуальное и психическое развитие,

состояние психического и физического здоровья.

Можно назвать несколько неблагоприятных факторов, которые привели к возникновению угрозы информационно-психологической безопасности, состоянию защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере.

Основным фактором является «информационный взрыв», или лавинообразное увеличение всех видов традиционной печатной информации (научной, научно-технической, экономической, научно-популярной, юридической, коммерческой, эстетической и т. д.). Еще бóльшими темпами развиваются электронные информационные ресурсы. Количественный рост информации привел к тому, что личность не может воспринять, осмыслить, систематизировать даже те источники информации, которые необходимы ей в профессиональной деятельности (для принятия управленческих, технологических, научных и иных решений). Этот фактор породил избыток, перенасыщение информационной среды. Большое количество информации, даже без учета ее качественных характеристик, отрицательно влияет на личность.

Другим неблагоприятным фактором, который влияет на психику современного человека, является значительное «загрязнение» информационной среды. Зарубежные авторы, изучающие качественную сторону потоков информации, считают, что информации не может быть много и информационный стресс вызывается не обилием информации, а большим количеством низкокачественной информации и неумением личности критически отсеивать, отбирать и перерабатывать информацию в интеллектуальный продукт (знания). Представитель этой концепции Б. Мильтон пришел к выводу, что информация — это лишь сырье, которое дает возможность вырабатывать знания, и что решения принимаются не на основе информации, а на основе знаний, мудрости, интуиции, понимания.

Говоря о качественной характеристике информационной среды, необходимо отдельно выделить в качестве негативного фактора, повлиявшего на нарушение информационно-психологической безопасности, широкое распространение способов управления поведением людей, манипуляций, информационно-психологических воздействий на индивидуальное и массовое сознание. Г. Грачев и И. Мельник различают несколько уровней применения манипулятивных технологий. Во-первых — это организованное влияние и психологические операции, осуществляемые в ходе реализации межгосударственной политики. Второй уровень информационно-психологического воздействия манипулятивного характера касается использования различных средств и технологий во внутриполитической борьбе, экономической конкуренции и деятельности организаций, находящихся в состоянии конфликтного противоборства. Наконец, третий уровень включает манипулирование людей друг другом в процессе межличностного взаимодействия. Экономические особенности рынка, прежде всего того, который имеет место в практике современной России и всего постсоветского пространства, буквально на глазах внес кардинальные изменения в поведение огромной части населения, подавляющее большинство которого оказалось не готово ни психологически ни морально к жестким правилам выживания по законам индивидуализма [4].

Несомненно, что решение проблемы обеспечения информационно-психологической безопасности должно носить комплексный системный характер и осуществляться на разных уровнях: нормативном, предполагающем создание органами государственной власти адекватной проблеме нормативной базы; организационно-институциональном, основанном на согласованной деятельности различных социальных институтов, и др. Однако начать следует с культурно-личностного уровня, требующего постоянного самовоспитания, самообразования личности, формирования необходимых личностных качеств для обеспечения информационной самозащиты. Поэтому остановим наше внимание на культурологическом подходе к информационно-психологической безопасности личности, базовым основанием которого является понятие «культура информационно-психологической безопасности».

Очевидно, что понятие «культура информационно-психологической безопасности» является частью наиболее общего понятия «культура информационной безопасности».

Для определения понятия культуры информационной безопасности мы проанализировали различные подходы к понятиям «культура» и «информационная безопасность» и выявили, что из существующих концепций сущности культуры (ведомственно-отраслевая, гуманистическая, информационно-семиотическая, духовно-

производственная, этно-археологическая, функционально-деятельностная и т. д.) наиболее широкими концепциями, обладающими эвристической ценностью в контексте предмета настоящей статьи, являются этно-археологическая и функционально-деятельностная.

В рамках этно-археологической концепции «культура» понимается как общая характеристика развития данного общества, народа, племени. Согласно этой концепции, культура размыта по всему телу социального организма, проникает практически во все его сферы: сферу материального производства (сферу экономики), сферу воспроизведения человеческого разума (семейно-бытовую сферу), сферу духовного производства (обеспечивающую производство и воспроизводство общественного сознания), систему организации и управления (политическую сферу). Например: античная культура, культура майя, культура неолита, культура охотников тропических лесов. С точки зрения функциональной (деятельностной, технологической) концепции культура — специфический способ организации и развития человеческой жизнедеятельности, представленный в продуктах материального и духовного труда, в системе социальных норм и учреждений, в духовных ценностях, в совокупности отношений людей к природе, между собой и к самим себе [6, с. 59—64].

Неоднозначно в современной науке трактуется и понятие информационной безопасности. Основываясь на «Доктрине информационной безопасности Российской Федерации» (2000) и на методологии деятельностного подхода, мы уточнили понятие информационной безопасности. Информационная безопасность — это состояние защищенности субъектов информационных отношений, включающее в себя качественную информационную среду (качество (оперативность, полнота, достоверность) потребляемой информации, защищенность субъектов от негативных информационных воздействий) (информационно-психологическая безопасность) и защищенность их информации (безопасность информации), обеспечивающее полное удовлетворение информационных потребностей субъектов. В данном определении мы учли все четыре национальных интереса в информационной сфере (соблюдение конституционных прав и свобод личности в информационной сфере, информационное обеспечение государственной политики, создание отечественной информационной индустрии и защита информации). В определении четко прослеживаются два вектора обеспечения информационной безопасности — это 1) обеспечение защищенности информации от субъектов информационных отношений; и 2) наоборот, — субъектов информационных отношений — от информации.

Опираясь на деятельностные концепции информационной безопасности и культуры, мы сформулировали определение культуры информационной безопасности**.** С технологической точки зрения культура информационной безопасности — это такой способ организации и развития человеческой жизнедеятельности в информационном пространстве, который обеспечивает качественную информационную среду (качество потребляемой информации, защищенность субъектов от негативных информационных воздействий) (информационно-психологическая безопасность) и защищенность их информации (безопасность информации). В конечном итоге только с помощью этого способа, имеющего дуальную структуру, можно достигнуть полного удовлетворения информационных потребностей субъектов.

Если смотреть с точки зрения теории интереса, культура информационной безопасности общества — это существующие в определенный период развития общества способы обеспечения интересов личности в информационной сфере, упрочения демократии, создания правового социального государства, достижения и поддержания общественного согласия, духовного обновления России, сохранения нравственных ценностей, утверждения в обществе идеалов высокой нравственности, патриотизма и гуманизма, развития многовековых духовных традиций России, пропаганды национального культурного наследия, норм морали и общественной нравственности, предотвращения манипулирования массовым сознанием, а также развития современных телекоммуникационных технологий, сохранения и развития отечественного научного и производственного потенциала. Очевидно, на разных этапах развития общества культура информационной безопасности имеет специфические качества.

Что касается культуры информационной безопасности личности, то она имеет более субъективный характер. Это такой способ организации и развития жизнедеятельности, при котором гражданин знает и способен реализовать свои конституционные права и свободы в информационной сфере (владеет технологиями доступа к государственным информационным ресурсам, может сохранить свою личную тайну, интеллектуальную собственность), умеет распознать негатив-

ные информационные воздействия, угрожающие его здоровью, и владеет технологиями защиты от них. Более подробно сущность понятия «культура информационной безопасности» обоснованы нами в [6].

Для определения понятия «культура информационно-психологической безопасности» вновь используем методологию деятельностного подхода, предполагающую анализ основных компонентов деятельности: цель, объект, субъект, процессы, средства, результат. Целью деятельности по обеспечению информационно-психологической безопасности, а, следовательно, и результатом данной деятельности выступает состояние защищенности от некачественной информации и негативных информационных воздействий. Объектом в условиях информационного взаимодействия с окружающей средой является субъект информационного взаимодействия. Соответственно, объектом выступает и общество, и государство, при этом процессы, средства обеспечения данной защищенности будут различными. Для обозначения условий информационного взаимодействия воспользуемся классификацией коммуникативных ситуаций, предложенной Г. В. Грачевым [5]. Данные условия взаимодействия Г. В. Грачев, называя коммуникативные ситуации, в которых на человека оказывается информационно-психологическое воздействие, делит на три группы: межличностные коммуникативные ситуации, контакт-коммуникационные ситуации, масс-коммуникационные ситуации. Следовательно, объект (личность) — субъект информационного взаимодействия. Осознание личностью субъектом обеспечения защищенности от информационных воздействий, представляющих угрозу, является одним из процессов данного обеспечения. Выдвижение в качестве результата данной деятельности «состояния защищенности от негативных информационных воздействий предполагает в буквальном смысле наличие угроз и противодействие им» [9, с. 20]. Следовательно, процессами обеспечения состояния защищенности субъекта выступают: выявление угроз информационно-психологической безопасности и противодействие им посредством использования субъектом знаний, умений, навыков (психических образований) в сфере информационно-психологической безопасности; памяти, критичности мышления (психических процессов); эмпатии и рефлексии (социально-психологической) (способов познания, понимания мира и себя как части мира).

Большое значение для определения культуры информационно-психологической безопасности имеет характеристика культуры, раскрывающая ее деятельностную сущность, — определение культуры как специфического способа человеческой деятельности, представленного в деятельностной концепции культуры Н. С. Злобина, М. С. Кагана, Э. С. Маркаряна и др. [7]. С этой точки зрения понятие деятельности является обобщающим как для характеристики культуры, так и для характеристики сущности человека как субъекта труда, познания и общения. Однако, опираясь на деятельностный подход, мы не ограничиваемся рассмотрением культуры личности через такие ее составляющие, как умственная, нравственная, правовая, физическая, информационная и т. п., то есть не через «вертикальный» разрез культуры человека, а предполагаем раскрытие данного феномена через комплекс трех его пластов: информационного, технологического, аксиологического. Это позволяет нам обосновать специфический подход к определению структурных компонентов (мотивационного, когнитивного, технологического, креативного) и функций (образовательной, коммуникативной, координирующей) культуры информационно-психологической безопасности.

Взяв за основу понятие культуры как специфического способа человеческой деятельности и понятие информационно-психологической безопасности как состояния защищенности субъектов информационного взаимодействия от некачественной информации и негативных информационных воздействий, сформулируем понятие культуры информационно-психологической безопасности. Культура информационно-психологической безопасности — структурно-уровневое, динамическое образование, представленное совокупностью структурных (мотивационного, когнитивного, технологического, креативного) и функциональных компонентов (образовательного, коммуникативного, координирующего), определяющее такой способ организации и развития жизнедеятельности, при котором субъект информационного взаимодействия осознает себя субъектом информационно-психологической безопасности, способен выявить угрозы информационно-психологической безопасности, владеет технологиями защиты от них, способен безопасно преобразовывать информационную среду [6].

В субъектах Российской Федерации ведется определенная работа, способству-

ющая повышению уровня культуры информационно-психологической безопасности. Так, в Челябинской области идет интенсивная профессионализация отрасли, создана система подготовки, переподготовки и повышения квалификации кадров по защите информации. Средства массовой информации освещают частные случаи манипуляций индивидуальным и массовым сознанием. Большую просветительскую работу ведет Управление по связям с общественными организациями Администрации г. Челябинска. Южно-Уральский центр медиаобразования ведет активную теоретическую и практическую работу в области медиаобразования: организует круглые столы, семинары, конференции, брифинги по вопросам медиаобразования; курсы повышения квалификации для действующих журналистов, руководителей и работников пресс-служб, сотрудников органов государственной власти и местного самоуправления; общественные семинары по информационной культуре для педагогов школ, детских домов, интернатов, социальных работников, неблагополучных групп населения. В организациях, на предприятиях крупного бизнеса региона стали обращать внимание на формирование корпоративной культуры, которая, безусловно, влияет на уровень их кадровой, а значит — информационной и в т. ч. — информационно-психологической безопасности. Ключевую, интегрирующую роль в формировании культуры информационной безопасности личности (а значит — и общества) в регионе сегодня играют кафедры вузов, которые реализуют образовательные программы по защите информации. К таким кафедрам относится кафедра «Информационная безопасность» Южно-Уральского государственного университета. Профессорско-преподавательский состав кафедры владеет соответствующими технологиями и обучает им не только будущих специалистов по защите информации, но и студентов других специальностей. Заметим, что речь идет не только о технологиях защиты личной конфиденциальной информации, но и о технологиях формирования собственной качественной, безопасной информационной среды личности: поиска, отбора, получения, передачи, хранения и аналитико-синтетической обработки и переработки информации, технологиях использования информационных продуктов и услуг на мировых информационных рынках, технологиях управления информационными процессами. Одним из приоритетных научных направлений кафедры является формирование критического мышления как средства защиты от негативных информационных воздействий в профессиональной деятельности, а также составляющей культуры информационно-психологической безопасности [1], разработана модель формирования культуры информационно-психологической безопасности [2] и др. Кафедрой организуются конференции, круглые столы, научные дискуссии и т. п.

Однако перечисленных мер, предпринимаемых в субъектах Российской Федерации для обеспечения информационно-психологической безопасности, недостаточно. Высок уровень информационных преступлений в регионах. Массовые случаи несанкционированного доступа к информации завершаются для собственников ее утратой и утечкой, при этом, несмотря на существование уголовной ответственности за компьютерные преступления, хакеры имеют социальный статус «героев», высокоинтеллектуальных, независимых, способных овладеть любыми, даже государственными секретами. Это свидетельствует, во-первых, о недостаточном развитии в регионах правовой культуры, а также лежащих в основе культуры информационно-психологической безопасности ценностных ориентаций, сущность которых составляет нетерпимость к информационным правонарушителям; во-вторых, о неспособности субъектов применить адекватные меры для обеспечения защищенности своей информации, содержащей различные виды тайн: личную, коммерческую, служебную, профессиональную и др. Оба аспекта — показатели низкой культуры информационной и в т. ч. — информационно-психологической безопасности в регионе.

Весьма тревожная ситуация сложилась в информационном пространстве регионов. Коммерциализация средств массовой информации привела к его существенному загрязнению. Недостаток информации о политике местных властей, большое количество искаженной и заведомо ложной информации, информации манипулятивного характера, исходящей от деструктивных общественных организаций, и т. п. — все это приводит к снижению уровня информационно-психологической безопасности субъектов информационных отношений в регионах. Это свидетельствует, во-первых, о недостаточности усилий региональных властей по решению проблем безопасности информационного пространства; во-вторых, о неспособности жителей регионов самостоятельно противостоять негативным информационным воздействиям; в-третьих,

о сформировавшихся в обществе ценностях, допускающих безответственное поведение в информационном пространстве, приводящее к резкому снижению качества последнего.

Уральский регион традиционно является опорой промышленности, вооружения и военной техники России. Здесь производится 45 % продукции топливной промышленности страны, 42 % продукции металлургического комплекса, около 10 % продукции машиностроения. Концентрация промышленного производства на Урале в 4 раза выше, чем в среднем по России. На обозримую перспективу он остается главным нефтегазодобывающим регионом, не имеющим аналогов как по запасам, так и по текущему уровню добычи углеводородов [8]. Поэтому обеспечение информационно-психологической безопасности в Уральском федеральном округе имеет ярко выраженную специфику и нуждается в особом внимании.

Выявленные проблемы информационно-психологической безопасности региона, их острота и необходимость решения подтверждаются результатами социологического опроса населения города Челябинска, проведенного силами кафедры «Информационная безопасность» Южно-Уральского государственного университета в конце 2009 года с целью изучения некоторых показателей состояния информационной безопасности горожан.

Всего было опрошено 896 респондентов старше 18 лет. При этом структура выборочной совокупности в основном соответствовала структуре генеральной совокупности. Были опрошены жители всех семи районов города (Центрального, Советского, Калининского, Металлургического, Тракторозаводского, Ленинского, Курчатовского), проживающие на разных улицах (как центральных, так и периферийных), в домах разного типа (старых, новых, коттеджных), в квартирах, расположенных на разных этажах.

Структура совокупности респондентов: 40 % — мужчины, 60 % — женщины; 32 % — до 30 лет, 25 % — 31—40 лет, 23 % — 41—50 лет, 12 % — 51—60 лет и 7 % старше 60 лет; 38 % респондентов имеют высшее образование, 32 % — среднее специальное, 19 % — среднее общее, 4 % — неполное среднее; 35 % респондентов имеют техническую специальность, 21 % — гуманитарную, 11 % — медицинскую, 21 % — экономическую, также были те, кто ответил «не имею специальность» — 8 %; 26 % опрошенных в настоящее время работают на производстве, 12 % — в сфере обслуживания, 10 % — в сфере торговли, 15 % обучаются в вузах, 11% являются домохозяйками/домохозяинами.

Первый блок вопросов был направлен на выявление представлений граждан Челябинской области об информационной безопасности и ее угрозах, источниках этих угроз. Анализ результатов социологического исследования показал, что всего 29 % опрошенных считают наиболее опасными угрозы в области психологической безопасности.

Однако при общении с малознакомыми людьми лишь 29 % респондентов открыты, стремятся узнать человека, достичь взаимопонимания; 48 % — осторожны, стараются держать все под контролем, пытаются понять истинные цели; 23 % придерживаются ритуального стиля общения. Полагаем в связи с этим, что низкий уровень опасности информационно-психологических угроз у опрошенных пока недостаточно отрефлексирован.

37 % респондентов указали, что были объектом негативных информационно-психологических воздействий и манипуляций. В основном эти воздействия исходили со стороны распространителей различных товаров и услуг (на это указали 46 % опрошенных), а также со стороны отдельных личностей (33 %) и СМИ (32 %). Немало и тех, кто указал в качестве источника негативных информационно-психологических воздействий и манипуляций деструктивные религиозные организации (23 %).

Проблемы информационно-психологической безопасности в субъекте подтверждает и тот факт, что защищенными чувствуют себя лишь 21 % опрошенных; 48 % ответили на этот вопрос отрицательно. Значительная часть респондентов не задумывались пока над данным вопросом (30 %).

Результаты анализа этого блока вопросов свидетельствуют об узком, стереотипном представлении об информационной безопасности, небезопасности регионального информационного пространства, что серьезно угрожает конституционным правам граждан субъекта в информационной сфере.

Второй блок вопросов был связан с методами и средствами обеспечения информационной безопасности.

Оказавшись в трудной жизненной ситуации, жители Челябинска чаще всего обращаются к родственникам и друзьям (64 % и 40 % соответственно), гораздо реже в милицию и в службу социальной защиты (13 % и 8 % соответственно), иногда — к коллегам (9 %) или в суд (7 %). Обеспечивать информационную безопасность граждан, по мне-

нию 37 % опрошенных, должны они сами, 24 % считают, что этим вопросом должно заниматься Правительство РФ, 16 % предположили, что это обязанность Президента РФ, также была названа ФСБ (15 %).

Однако, несмотря на убежденность в необходимости самозащиты от негативного влияния информации, знаний о том, как это делать, у опрошенных нет. Так, на вопрос о влиянии большого количества информации на человека всего 36 % ответили, что огромное количество информации требует избирательности и критичности. Это небольшой процент жителей города, осознающих для себя опасность угроз со стороны информации и необходимость развития критического восприятия информации.

Не зная методов информационной самозащиты, 76 % челябинцев ничего не знают и о мерах, которые принимает руководство Челябинской области для обеспечения информационной безопасности населения нашего региона. Жители города Челябинска практически не знают о региональной политике информационной безопасности и стараются обеспечить ее сами, не надеясь на органы власти. Кстати, по результатам инициативного всероссийского опроса ВЦИОМ, проведенного в сентябре 2009 года и в рамках которого опрошено 1600 человек в 140 населенных пунктах, краях и республиках России, 29 % плохо представляют себе задачи и функции ФСБ, 48 % — знают о функциях ФСБ лишь в общих чертах. Еще более неизвестен в России Национальный антитеррористический комитет: плохо представляют себе его задачи и функции 37 % опрошенных и знают о нем в общих чертах 42 % [3]. Это свидетельствует о проблемах информационного обеспечения политики информационной безопасности не только в Челябинской области, но и в России в целом. Налицо также низкая культура информационно-психологической безопасности жителей региона.

Очевидно, что даже самый беглый взгляд на результаты социологического опроса, связанного с выявлением некоторых показателей уровня информационной безопасности, свидетельствует о небезопасности информационного пространства области и низком уровне культуры информационно-психологической безопасности граждан для реализации собственных конституционных прав в информационной сфере; недостаточном уровне информационного обеспечения региональной политики безопасности [6, с. 25—30].

Для решения проблемы формирования культуры информационной безопасности в Уральском федеральном округе необходимо принятие не фрагментарных, а системных мер, реализованных в форме концептуального документа — Концепции формирования культуры информационно-психологической безопасности (или кибербезопасности), а также Программы реализации этой Концепции. В данных документах должны найти свое отражение пути решения институциональных проблем региональной информационной безопасности: организационная раздробленность отрасли в регионе и, как следствие, — жесткие ведомственные барьеры при решении комплексных проблем информационной безопасности, к каковым относится и информационно-психологическая безопасность; стереотипичные акценты на техническую защиту информации в деятельности органов государственной власти и невнимание вопросам гуманитарным (патриотизация, духовное развитие общества, качество информационной среды), координация этой деятельности со стороны органов власти региона. Следует предпринять немалые усилия по широкомасштабной популяризации знаний культуры информационной безопасности в субъектах Федерации, входящих в УрФО. Только в этом случае возможна успешная реализация «Стратегии национальной безопасности Российской Федерации до 2020 года».

Таким образом, на основе анализа научной литературы было выявлено, что культура информационно-психологической безопасности субъекта практически не изучена: отсутствует научно-обоснованное понятие, не разработана целостная система ее обеспечения. Между тем, потребность в изучении этого нового для информационного общества явления весьма высока, что подтвердили результаты проведенного кафедрой «Информационная безопасность» ЮУрГУ социологического исследования, выявившего недостаточный уровень информационно-психологической безопасности жителей города Челябинска. На основе системно-деятельностного подхода к понятиям культуры и информационно-психологической безопасности сформулировано определение культуры информационно-психологической безопасности, которое должно определять содержание деятельности по ее формированию у субъектов информационного взаимодействия. К основным содержательным компонентам культуры информационно-психологической безопасности относятся: самоосознание субъектом информационного взаимодействия субъектом информационно-психологической безопасности, его способность выявлять угрозы

информационно-психологической безопасности, владеть технологиями защиты от них, мотивация субъекта безопасно преобразовывать информационную среду. Названные содержательные компоненты должны найти отражение в региональной Концепции и Целевой программе формирования культуры информационной безопасности (культуры кибербезопасности) в Уральском федеральном округе либо в подобных документах в субъектах Федерации, входящих в состав УрФО.

Литература

1. *Астахова, Л. В.* Критическое мышление как средство обеспечения информационно-психологической безопасности личности : монография / Л. В. Астахова, Т. В. Харлампьева ; под научн. ред. Л. В. Астаховой. — М. : РАН, 2009. — 141 с.
2. *Ахметвалиева, А. А.* Модель формирования культуры информационно-психологической безопасности будущих специалистов в процессе подготовки в вузе / А. А. Ахметвалиева // Вестник Челябинского государственного педагогического университета. — 2009. — № 12. — С. 5—13.
3. ВЦИОМ (электронный ресурс)//http://wciom.ru/arkhiv/tematicheskii-arkhiv/item/single/12600.html
4. *Грачев, Г.* Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия / Г. Грачев, И. Мельник. — [Электронный ресурс] // www.philosophy.ru/iphras/library/manipul.html.
5. *Грачев, Г. В.* Личность и общество: информационно-психологическая безопасность и психологическая защита / Г. В. Грачев. — Волгоград : Издатель, 2004. — 336 с.
6. Информационная безопасность региона: традиции и инновации : монография / под науч. ред. Л. В. Астаховой. — Челябинск : Издательский центр ЮУрГУ, 2009. — 269 с.
7. *Лурье, С. В.* Психологическая антропология: история, современное состояние, перспективы. — М. : Академический проект ; Деловая книга, 2005. — 624 с.
8. Совет безопасности Российской Федерации: официальный сайт (электронный ресурс) //http://www.scrf.gov.ru/news/475.html
9. *Тер-Акопов, А. А.* Безопасность человека: Социальные и правовые основы. — М. : Норма, 2005. — 272 с.

АСТАХОВА Людмила Викторовна, д. п. н., профессор, зав. кафедрой «Информационная безопасность» ЮУрГУ.

ASTAKHOVA Lyudmila Viktorovna, Doctor of Education, Professor. South Ural State University.

УДК 316.777:004.056 + 351/354:004 + 005.922.1
ББК Х401.114 + Х408.135

А. Болгарский

Защита информации в государственных информационных системах

A. Bolgarsky

Information protection in state information systems

В статье рассматривается актуальность и понятие государственных информационных систем, виды обрабатываемой и защищаемой в них информации, виды угроз этой информации, а также нормативные акты, регулирующие вопросы защиты информации в государственных информационных системах.

***Ключевые слова**: государственная информационная система, защита информации, угрозы, способы защиты.*

The paper covers the concept of state information systems and their importance, types of information processed and protected within these systems, types of threats to information security, as well as statutory regulations governing the issues related to information security and protection in state information systems.

***Keywords**: State information system, information protection, threats, protection methods.*

Развитие современного общества невозможно без совершенствования приемов, способов и методов применения технических и программных средств при обработке информации, объем которой постоянно нарастает. Другими словами, совершенствование информационных технологий является объективной реальностью нашего времени и способствует развитию информационных систем и в целом повышению уровня информатизации во всех сферах деятельности общества.

В настоящее время в Российской Федерации проводится широкий комплекс социально значимых реформ. Активно осуществляются реформы образования, здравоохранения и др. Особое значение придается вопросу повышения уровня информатизации органов государственной власти. Развитие информационных технологий в информационных системах органов государственной власти непосредственно ведет к актуализации вопроса защиты информации, обрабатываемой в них.

В соответствии со статьей 6 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон № 149-ФЗ) обладателем информации, которым может быть гражданин (физическое лицо), юридическое лицо, муниципальное образование, субъект Российской Федерации, Российская Федерация, должны быть приняты меры по защите информации.

В соответствии с ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» под ***защитой информации*** понимают деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

В соответствии со статьей 16 Закона № 149-ФЗ защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

— обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а

также от иных неправомерных действий в отношении такой информации;

— соблюдение конфиденциальности информации ограниченного доступа,

— реализацию права на доступ к информации.

Другими словами, реализуя меры по защите, оператор должен достигнуть такого состояния защищенности информации в информационной системе, при котором обеспечивается ее ***конфиденциальность***, ***доступность*** и ***целостность***.

Используемые здесь общетехнические понятия можно рассматривать в следующих значениях:

конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

доступность информации — состояние информации, при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно;

целостность — состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

В соответствии со ст. 13 Закона № 149-ФЗ к ***государственным информационным системам*** относятся федеральные информационные системы и региональные информационные системы, созданные соответственно на основании федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

Здесь необходимо отметить, что установленные требования к государственным информационным системам распространяются также и на ***муниципальные информационные системы***, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.

В государственных информационных системах обрабатывается различная информация. В зависимости от категории доступа она подразделяется на ***общедоступную информацию***, а также на информацию, доступ к которой ограничен федеральными законами (***информация ограниченного доступа***).

Защита информации, составляющей ***государственную тайну***, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим ***служебную тайну и иную тайну***, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Меры по обеспечению безопасности ***персональных данных*** при их обработке, в том числе в информационных системах персональных данных, установлены Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Обязанности обладателя информации, оператора информационной системы, по защите информации определены ст. 16 Закона № 149-ФЗ, где говорится, что в случаях, установленных законодательством, он обязан обеспечить:

предотвращение несанкционированного доступа (далее — НСД) к информации;

своевременное обнаружение фактов несанкционированного доступа к информации;

недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

постоянный контроль за обеспечением уровня защищенности информации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (***ФСБ России***), и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (***ФСТЭК России***), в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Важным замечанием является то, что требования о защите ***общедоступной информации*** могут устанавливаться только для обеспечения целостности и доступности.

То есть, общедоступная информация, обрабатываемая в информационных системах, также подлежит защите, как и информация ограниченного доступа, например, содержащая сведения, составляющие государственную тайну. Но для обеспечения безопасности общедоступной информации не требуется обеспечение ее конфиденциальности.

Требования по защите общедоступной информации основываются на тех угрозах безопасности информации, которые имеются для таких информационных систем. Без-

условно, актуальность каждой возможной угрозы для конкретной информационной системы определяется индивидуально, вместе с тем, можно выделить типовые угрозы для данных информационных систем. Это, прежде всего, угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на:

содержание информации, в результате которого осуществляется изменение информации или ее уничтожение;

программные или программно-аппаратные элементы информационной системы, в результате которого осуществляется блокирование информации.

Такими угрозами могут быть:

угрозы удаленного доступа, которые реализуются с использованием протоколов сетевого взаимодействия;

угрозы создания нештатных режимов работы программных и программно-аппаратных средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т. п. — угроза «Отказ в обслуживании»;

угрозы внедрения вредоносных программ (программно-математические воздействия):

программных закладок;

классических программных (компьютерных) вирусов;

вредоносных программ, распространяющихся по сети (сетевых червей);

других вредоносных программ, предназначенных для осуществления НСД.

Источниками угроз безопасности информации, обрабатываемой в государственных информационных системах, могут быть как внутренние нарушители, так и внешние.

В целях обеспечения информационной безопасности Российской Федерации, в том числе защиты общедоступной информации, обрабатываемой в информационных системах, имеющих подключение к информационно-телекоммуникационным сетям (далее — ИТКС) международного информационного обмена (например, к сети Интернет), государственные органы должны использовать только средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в ФСБ России и (или) получившие подтверждение соответствия в ФСТЭК России. Это требование определено пунктом 1 Указа Президента Российской Федерации от 17 марта 2008 г. № 351.

В соответствии с постановлением Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям» ФСБ России и ФСТЭК России издали совместный приказ от 31 августа 2010 г. № 416/489, в котором утверждены требования о защите информации, содержащейся в информационных системах общего пользования.

Данным приказом определено, что информационные системы общего пользования подразделяются на два класса. Для каждого класса установлены соответствующие требования к защите информации. Одним из основных является обязательность использования сертифицированных ФСБ России (для 1 класса) и ФСТЭК России (для 2 класса) средств защиты информации.

Методы и способы защиты информации определяются оператором информационной системы самостоятельно.

Таким образом, реализация в государственных информационных системах необходимых мер по защите обрабатываемой в них информации позволит создать условия для повышения качества и эффективности государственного управления, увеличения конкурентоспособности экономики и уровня развития общества, а также обеспечит реализацию законных интересов граждан при информационном взаимодействии с органами государственной власти.

БОЛГАРСКИЙ А. И., руководитель Управления Федеральной службы по техническому и экспортному контролю по Уральскому федеральному округу.

BOLGARSKIY A. I., Head of Administration of the Federal Service for Technical and Export Control for the Urals Federal District

УДК 004.056.53 + 005.922.1
ББК Ч23:Х401.114

М. С. Политов

Оценка уровня защищенности информационных систем, ее достоверность и прогнозирование результатов

M. S. Politov

Estimating security level of information systems, its reliability and results forecasting

В статье сделана попытка найти наиболее эффективную модель, опирающуюся на достоверные данные, для описания динамики уровня защищенности информационной системы. На основе проведенного анализа существующих и успешно применяющихся сегодня методик был сформулирован и предложен новый подход к построению прогнозных моделей, основанный на применении теории временных рядов.

Ключевые слова: *информационная безопасность, защищенность, уязвимость, критерии защищенности, прогнозная модель, прогнозирование, оценка уровня защищенности, временные ряды, достоверность.*

In this article we attempt to find the most efficient model, based on reliable data to describe the information systems security level dynamics. Based on the analysis of existing and successfully today applied techniques has been formulated and proposed a new approach to constructing forecasting models based on the time series theory.

Keywords: *information security, security, vulnerability, protection criteria, forecasting model, forecasting, security level estimating, time series theory, reliability.*

Введение

Одной из основных проблем современного информационного общества является значительное отставание уровня информационной безопасности от уровня и темпов развития информационных технологий. Бурное развитие информационных технологий открыло новые возможности для бизнеса, однако привело и к появлению новых угроз.

1. Актуальность

Современные информационные системы (ИС), находящиеся в производственной эксплуатации, включают в себе функции защиты обрабатываемых в них данных. Однако динамика изменения количества инцидентов в этой области свидетельствует о наличии ряда нерешенных проблем. В частности, при создании современных программных продуктов производители в первую очередь стремятся оптимизировать свои решения по двум основным критериям: функциональные возможности, которые должны превосходить ближайших конкурентов, и скорость разработки. При таком подходе вопросы качества и безопасности программного кода уходят на второй план. В итоге ошибки и недоработки недоотлаженных систем приводят к случайным и преднамеренным нарушениям основных свойств информационной безопасности. Так, например, за первые полгода после выпуска серверной операционной системы Microsoft Windows Server 2003 было обнаружено 14 уязвимостей, 6 из которых являются критически важными [1]. Несмотря на то что со временем специалисты компании Microsoft выпустили пакеты обновлений, устраняющие обнаруженные недостатки, существенный процент пользователей уже успел пострадать от связанных с этим инцидентов неправомерного доступа. Аналогичная ситуация имеет место и с программными продуктами других фирм. Пока

не будет решена задача своевременного выявления и устранения уязвимостей в эксплуатируемых ИС, недостаточный уровень защищенности станет серьезным тормозом в развитии глобальных информационных технологий.

2. Постановка задачи

С учетом изложенного положения дел в области защищенности информационных систем, в данной статье рассмотрено построение и использование прогнозных моделей на основе теории временных рядов для оценки и прогнозирования уровня защищенности ИС. Данный метод построен на статистической обработке достоверной информации, получаемой из международных баз уязвимостей и от производителей конкретных продуктов и систем. Стоит отдельно отметить, что данный метод имеет как минимум одно неоспоримое преимущество среди подобных прогнозных моделей, которое заключается в неоспоримой достоверности используемых исходных данных, в то время как распространенные сегодня системы оценок в основе своей используют экспертные показания и данные, которые существенно разнятся от эксперта к эксперту. Т. е. для оценки уязвимости программно-технического продукта предлагается использовать статистику обнаруженных и уже классифицированных по общепринятым меркам уязвимостей в привязке к конкретной версии информационной системы.

3. Методика исследования

Выделяют две основные цели использования мониторинга в научно-практической деятельности: предупреждение и прогнозирование [2]. В обоих случаях мониторинг основан на систематическом слежении за определенными характеристиками исследуемого процесса. Задача предупреждения — в предотвращении нежелательных отклонений по важным параметрам. Примерами мониторинговых систем такого рода применительно к сфере информационных технологий являются системы противодействия кибератакам, подробно рассмотренные в [3]. Собранные статистические данные в ходе мониторинга могут использоваться для эффективного прогнозирования развития исследуемого процесса.

Для создания предлагаемой прогнозной модели [4] на основе теории временных рядов необходимо ввести следующие определения и допущения.

1. Жизненный путь программно-технического средства оценивается в количестве выпущенных производителем версий и модификаций.

2. Подсчет количества версий ведется не по числу реально используемых версий, а исходя из формальной системы образования порядкового номера версии. При этом не учитывается факт существования/отсутствия каждой отдельной.

3. Виды и типы уязвимостей классифицируются следующим образом:

— *Low* — уязвимости типа «поднятие локальных привилегий», но не до local system;

— *Midle* — уязвимости, мешающие нормальному функционированию системы и приводящие к возникновению DoS; уязвимости, приводящие к поднятию локальных привилегий до local system;

— *High* — уязвимости, позволяющие злоумышленнику получить удаленный контроль над системой.

4. Уровень защищенности информационной системы оценивается по отношению общего количества уязвимостей каждого класса к общему количеству версий системы.

Построение прогнозной модели выполнено на примере web-сервера Apache (см. рис. 1).

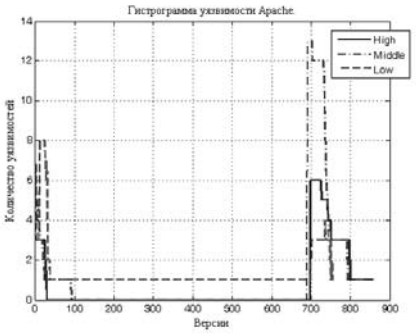


Рис. 1. Уровень уязвимости для различных версий web-сервера Apache

Как известно, смена основных номеров версий программного обеспечения связана с существенными изменениями кода и функциональными преобразованиями. В пределах этих версий идет доработка уже заложенного функционала и исправление ошибок.

Для прогнозирования числа уязвимостей в будущих версиях web-сервера Apache была применена теория временных рядов и выполнен анализ полученных данных. Как известно, временной ряд есть последовательность измерений, выполненных через определенные промежутки времени. В нашем случае шкала версий программного продукта рассматривалась как шкала времени.

Использовалась классическая модель временного ряда, состоящая из четырех компонент:

тренда — общей тенденции движения на повышение или понижение;

циклической составляющей — колебания относительно основной тенденции движения;

случайной составляющей — отклонения от хода отклика, определяемого трендовой, циклической и сезонной составляющими. Данная составляющая связана с ошибками, измерениями или влияниями случайных величин.

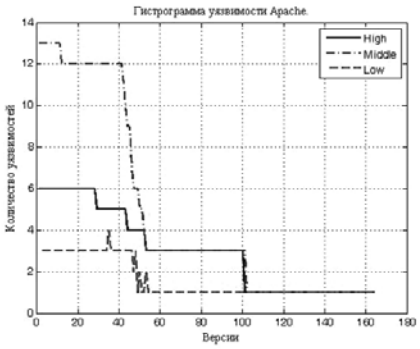


Рис. 2. Версионная уязвимость второй версии web-сервера Apache

Известны различные модели регрессионного анализа, позволяющие определить функциональную зависимость трендовой составляющей. В рассматриваемой ситуации был выбран метод, основывающийся на подборе максимального соответствия показателей математической модели показателям моделируемой системы. Анализ опыта таких компаний, как General Motors и Kodak, при выборе аппроксимирующей модели позволил выбрать за основу трендовой составляющей степенной закон. Основываясь на типовых элементах процесса для рассматриваемого множества примеров, выбран следующий вид трендовой функции:

$$y(x) = b_0 \cdot b_1^x .$$

Или же, применимо к нашему случаю:

High $y(x) = 7.2218 \cdot 0,9873^x - 0.4958 \cdot 0,9983^x \cdot \cos(0,1021 \cdot x + 0,3689).$

Middle $y(x) = 16.5603 \cdot 0,9807^x + 1.5442 \cdot 0,9955^x \cdot \cos(0,1022 \cdot x + 3,0289).$

Low $y(x) = 3.5053 \cdot 0,9887^x + 0.3313 \cdot 0,9967^x \cdot \cos(0,1011 \cdot x + 2.9589).$

Из графиков экспериментальных данных (см. рис. 2, 3) следует, что амплитуда колебаний затухает с течением времени. Данный процесс отражает работу над ошибками компанией-производителем по выпуску патчей к своей системе.

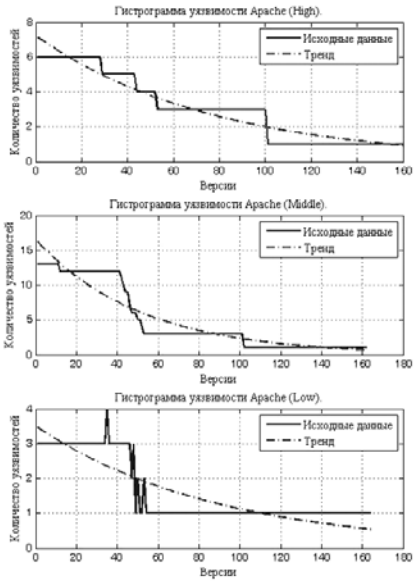


Рис. 3. Кривые основного тренда уязвимости в зависимости от версии

Для аппроксимации циклической составляющей, описывающей колебательный процесс устранения уязвимостей, которые вносятся вновь применяемыми патчами, была выбрана функция следующего вида:

$$y(x) = b_0 \cdot b_1^x + d \cdot f^x \cdot \cos(c \cdot x + a).$$

В результате моделирования описываемых процессов были получены следующие формулы итоговых аппроксимирующих функций:

High $y(x) = 7.2218 \cdot 0,9873^x - 0.4958 \cdot 0,9983^x \cdot \cos(0,1021 \cdot x + 0,3689).$

Middle $y(x) = 16.5603 \cdot 0,9807^x + 1.5442 \cdot 0,9955^x \cdot \cos(0,1022 \cdot x + 3,0289).$ (1)

Low $y(x) = 3.5053 \cdot 0,9887^x + 0.3313 \cdot 0,9967^x \cdot \cos(0,1011 \cdot x + 2.9589).$

Адекватность предлагаемых математических зависимостей исходным данным предлагается проверить критерием Пирсона.

Проверка гипотезы показала, что исходные временные ряды соответствуют рядам, построенным по функциям (1) (см. рис. 4).

Для вычисления статистики Пирсона была использована следующая формула:

$$\chi^2 = N \sum_{i=1}^{k} \frac{(p_i^{emp} - p_i^{teor})^2}{p_i^{teor}},$$

где p_i^{teor}, p_i^{emp} — вероятность попадания уровня уязвимости в i-й интервал в исходном и теоретическом рядах;

N — суммарное число уязвимостей версий в исходном временном ряду;
k — количество точек временного ряда.

В результате были получены следующие значения χ^2 (табл. 1). Согласно таблице значений для критерия Пирсона при заданном количестве степеней свободы k – 1 = 160 и уровне значимости α = 0,01 получаем следующее значение для $\chi^2_{табл}$ = 204,5301. Так как все $\chi^2 < \chi^2_{табл}$, поэтому гипотезы H_0 принимаются на самом минимальном уровне значимости α = 0,01.

Таблица 1

Класс уязвимости	χ^2
High	10,8327
Middle	37,7546
Low	18,1643

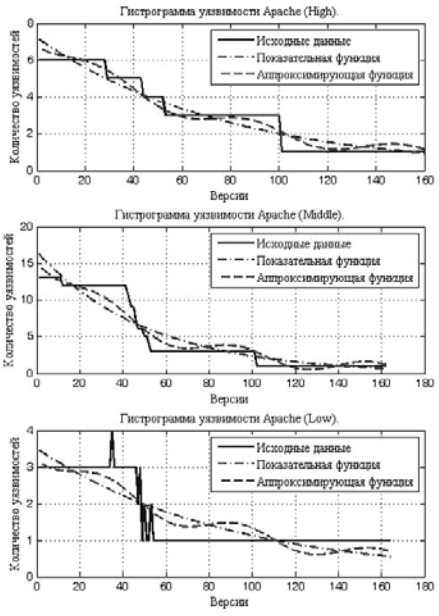


Рисунок 4 — Аппроксимация кривых уязвимостей на базе выбранных функций

ми табличными данными, и теоретические (1) соответствуют друг другу.

Для прогнозирования будущих значений предлагается применить полученные зависимости временных рядов (1) с учетом номера версии ИС.

Точность предложенного метода оценивалась на основе сравнения среднего абсолютного отклонения функций временного ряда и среднего абсолютного отклонения функций экспертного метода. Согласно ряду научных трудов [5], в первом приближении экспертная оценка может быть представлена либо линейной, либо степенной функцией (см. рис. 4), отражающей основной тренд процесса. Среднее абсолютное отклонение (MAD) определяется следующей формулой:

$$MAD = \frac{\sum_{i=1}^{n} |y_i - \tilde{y}_i|}{n},$$

где y_i — вычисленное в i-й точке значение временного ряда ;
$\tilde{y}_i$ — наблюдаемое в i-й точке значение ряда;
n — количество точек временного ряда.

Достоверность предлагаемого метода определена по формуле:

$$D = \frac{k}{n},$$

где k — количество точек рассматриваемой функциональной зависимости, попадающих в десятипроцентный интервал относительно значений исходного временного ряда;
n — общее количество точек временного ряда.

Как видно из табл. 2 предложенный в работе метод позволяет получить оценку в два раза точнее экспертного оценивания и увеличить достоверность прогноза на 20 %.

Таблица 2

Класс уязвимости	MAD			Достоверность	
	Линейная	Степенная	Степенная функция с циклической составляющей	Степенная	Итоговая
High	0,5737	0,5250	0,3882	0,675	0,8875
Middle	2,1398	1,5542	1,0730	0,7037	0,821
Low	0,5568	0,4630	0,3921	0,622	0,7134

Таким образом, доказано, что для минимального уровня значимости α = 0,01 по критерию согласия Пирсона функциональные зависимости, представленные исходны-

Выводы

1. Проведенный анализ существующих проблем в области оценки и прогнозирования уровня защищенности инфор-

мационных систем выявил актуальность создания гибких прогнозных моделей, описывающих изменение значений показателей безопасности информационных систем.

2. Предложен подход к оценке уровня защищенности информационных систем, основанный на достоверной информации, а не на субъективных знаниях экспертов. Также особенностью данного подхода является его эффективность при применении к достаточно «молодым» ИС, что обосновано использованием теории временных рядов.
3. В качестве примера разработана прогнозная модель изменения уровня защищенности web-сервера Apache на основе теории временных рядов, доказана ее адекватность и эффективность использования.

Литература

1. Цифры на стороне Microsoft [Электронный ресурс] //SecurityLab — Российский интернет-портал об информационной безопасности. (http://www.securitylab.ru/news/213467.php)
2. *Майоров, А. Н.* Мониторинг как научно-практический феномен [Текст] / А. Н. Майоров // Школьные технологии. — 1998. — № 5. — С. 52—56.
3. *Биячуев, Т. А.* Проблемы защиты киберпространства и пути их решения [Текст] / Т. А. Биячуев. — СПб. : СПб ГУ ИТМО, 2004. — С. 34—38.
4. *Политов, М. С.* Экспериментально-аналитический метод оценки и прогнозирования уровня защищенности информационных систем на основе модели временных рядов : дис. … канд. техн. наук : 05.13.19 [Текст] / М. С. Политов. — Уфа, 2010. — 145 с. : ил. РГБ ОД, 61 10-/1544.
5. *Сидельников, Ю. В.* Системный анализ технологии экспертного прогнозирования [Текст] / Ю. В. Сидельников. — М. : МАИ, 2007. — С. 231—270.

ПОЛИТОВ Михаил Сергеевич, зам. нач. вычислительного центра ЧелГУ, специалист по защите информации, канд. техн. наук. E-mail: msp@csu.ru

POLITOV Mikhail Sergeevich, Deputy Head of Data Center of Chelyabinsk State University (ChelGU), specialist in information protection, Candidate of Legal Sciences.
E-mail: msp@csu.ru

УДК 004.056;004.7.072.4
ББК 3973-018.2

Д. И. Дик

Применение мутационного анализа для оценки качества тестирования межсетевых экранов

D. I. Dik

Application of mutation analysis in assessing the quality of firewall testing

В статье предлагается метод контроля качества тестов для регламентного тестирования межсетевых экранов. Метод тестирования основан на применении мутационного тестирования к спискам контроля доступа межсетевого экрана. Следствием применения метода является повышение полноты покрытия политик безопасности межсетевых экранов тестами и устранение ошибок в тестах.

***Ключевые слова**: межсетевой экран, списки контроля доступа, мутационное тестирование.*

The paper offers a method to audit the quality of tests used in scheduled firewall testing. The proposed method is based on mutation testing applied to a firewall access control lists. This method results in more extensive coverage of firewall security policies by tests and eliminates test errors.

***Keywords**: firewall, access control lists, mutation testing.*

Поскольку межсетевые экраны находятся на границе сетей и являются узловой точкой доступа, они являются одним из ключевых элементов системы защиты информации. Организации, использующие межсетевые экраны, должны быть уверены в правильности и надежности функционирования основной точки доступа. Эта проблема решается при помощи тестирования межсетевых экранов. Необходимость тестирования межсетевых экранов также закреплена в соответствующих нормативных документах[1].

Одной из важнейших задач тестирования является проверка выполнения межсетевым экраном заданной политики безопасности:

1) проверка выполнения требований безопасности:

— выполнение функций контроля доступа;

— контроль соответствия записей в журнал регистрации;

— контроль подсистемы генерации сигналов тревоги;

— контроль доступности;

2) проверка требуемой функциональности:

— проверка выходящих служб (во внешний мир);

— проверка входящих служб (в защищаемую сеть);

— проверка служб, необходимых для взаимодействия с Интернетом.

Для проведения тестирования межсетевых экранов необходимо сформировать набор тестов, которые призваны показать правильность (или неправильность) функционирования межсетевого экрана. Однако здесь возникает серьезная проблема контроля правильности тестов. Таким образом, мы имеем дело с известной философской проблемой «Quis custodiet ipsos custodes?», которую можно перевести как «Кто охраняет охранников?».

Метод мутационного тестирования зародился в 70-х годах прошлого века и получил первое практическое применение в 80-х. Мутационное тестирование появилось как метод тестирования программного обеспечения, заключающийся во внесении неболь-

ших изменений в исходный код программы. Отсутствие ошибок и неверных результатов при тестировании измененной программы на наборе тестов может означать низкое качество предоставленного набора тестов (неполноту или ошибочность).

Для применения мутационного тестирования выбирается набор мутационных операторов, которые по одному применяются к исходному коду. Мутационные операторы обычно включают в себя удаление строки кода, замену одного оператора другим, замену переменной на другую переменную того же типа, а также другие характерные для программистов ошибки[2].

Мутационные подходы нашли применение не только для контроля корректности и полноты тестов при разработке программного обеспечения.

Так, при тестировании систем защиты находит широкое применение мутация данных для тестирования интерфейсов на устойчивость. Под мутацией данных подразумевается ситуация, когда на вход интерфейса поступают специальным образом измененные данные. Вследствие чего код обработки данных, поступающих на интерфейс, может повести себя опасным образом.

На рис. 1 показаны методы внесения возмущений в среду, в которой работает приложение[3].

В последние время наметилась тенденция использовать мутационный анализ для контроля тестов, используемых для тестирования политик доступа в трехуровневых архитектурах для моделей ролевого разграничения доступа.

Так, Т. Ши и Е. Мартин[4] применили мутации для тестирования XACML. XACML является Oasis стандартом XML синтаксиса для определения политик безопасности. Было предложено несколько операторов мутации. Большинство из этих операторов зависят от платформы и связаны со способами, которыми XACML выражает политики и правила. Вот некоторые примеры операторов:

– RTT: Удаляет конкретный объект политики, после чего политика применяется ко всем запросам;

– CPC: Изменяет сочетание алгоритмов (эти алгоритмы позволяют решать, какие правила/политики применяются);

– CRE: Изменяет тип правила (Отвергать становится Допускать и Допускать становится Отвергать).

Фактически часть из операторов (таких как RTT) имитирует все возможные синтаксические ошибки XACML синтаксиса. Другие операторы (например, CPC и CRE) имитируют семантические ошибки.

Т. Мулхай, Дж. Л. Траон и Б. Боудри[5] применили мутационный анализ для проверки качества тестов в рамках OrBAC (Organization Based Access Control) моделей. В OrBAC правило безопасности может быть разрешением, запрещением или обязатель-

Рис. 1. Методы возмущения среды для обнаружения недостатков защиты и надежности

ством. Правило имеет пять параметров (названных категориями): организация, роль, деятельность, вид и контекст. Чтобы увеличить агрегирование при определении правил безопасности, OrBAC позволяет определение иерархий для категорий. В этом случае, правила, определенные для категорий высокого уровня, наследуются подкатегориями.

Предложено ряд операторов мутации, которые приспособлены к OrBAC. Вот некоторые примеры:

— PPR: заменяет разрешение запрещением;

— CRD: заменяет контекст правила другим;

— APD: заменяет область действия правила одним из ее потомков;

— ANR: добавляет новое правило.

Как и в предыдущей статье, некоторые операторы связаны с моделью OrBAC.

Т. Мулхай, Ф. Флурей и Б. Боудри[6] предприняли попытку построить общую метамодель для различных формализмов представления правил безопасности.

Предложены операторы мутаций, независимые от любого формализма безопасности:

— RTT: выбирает правило и заменяет тип правила на другой при условии совпадения параметров;

– PPR: выбирает правило из набора правил и затем заменяет один параметр другим параметром;

– ANR: добавляет новое правило, которое ранее не определено;

– RER: выбирает правило и удаляет его;

– PPD: выбирает правило, которое содержит параметр, имеющий дочерние параметры (на основе определенной иерархии параметров) и заменяет параметр одним из потомков.

В данной работе предлагается применить мутационный анализ к спискам контроля доступа (ACL) межсетевых экранов.

Межсетевой экран обеспечивает защиту посредством фильтрации информации, т. е. ее анализа по совокупности критериев и принятия решения о ее распространении. Межсетевой экран просматривает пакеты, проходящие через него в обоих направлениях, и принимает решение о допуске или уничтожении пакетов. Таким образом, межсетевой экран реализует одну точку защиты между двумя сетями — он защищает одну сеть от другой.

Каждый пакет исследуется на соответствие множеству правил. Эти правила устанавливают разрешение связи по содержанию заголовков сетевого и транспортного уровней модели TCP/IP, анализируется и направление передвижения пакета.

Фильтры пакетов контролируют:

— физический интерфейс, откуда пришел пакет;

— IP-адреса источника и назначения;

— тип протокола транспортного уровня (TCP, UDP, ICMP);

— порты источника и назначения.

Для реализации процесса фильтрации пакетов применяются правила, называемые списками контроля доступа (Access Control List, ACL или просто Access List, AL).

В качестве примера рассмотрим реализацию фильтров в маршрутизаторах компании Cisco[7].

Список контроля доступа содержит перечень элементов в заголовках пакетов, которые будут проверяться. Маршрутизаторы Cisco определяют списки доступа как последовательный набор запрещающих и разрешающих условий. Каждый пакет проверяется на соответствие правилам списка. Если пакет соответствует правилу, то он отбрасывается (если это запрещающее правило) или принимается (если это правило разрешающее). Если пакет соответствует правилу, то он уже не будет проверяться на соответствие остальным правилам. Поэтому порядок пра-

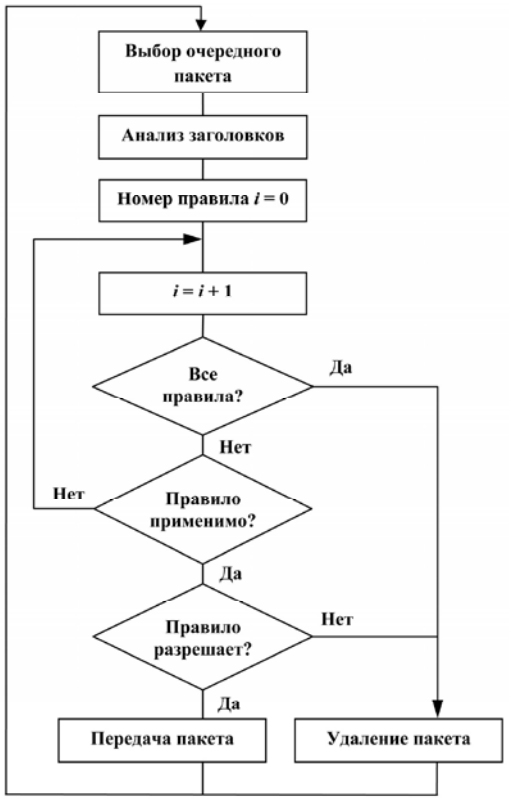


Рис. 2. Схема обработки пакетов при фильтрации

вил в списке доступа играет важную роль. Если ни одно из правил не было применено, то пакет удаляется.

Таким образом, обработка дейтаграммы при фильтрации может быть представлена в виде схемы, приведенной на рис. 2.

Маршрутизаторы Cisco поддерживают нумерованные и именованные списки доступа. Для протокола IP (в дальнейшем будет рассматриваться только этот протокол) и нумерованные, и именованные списки доступа подразделяются на две категории: стандартные (*standard*) и расширенные (*extended*). В качестве критерия отбора в стандартном списке доступа выступает IP-адрес источника, тогда как расширенный список может осуществлять сравнение с IP-адресами источника и пункта назначения, типом IP-протокола, портами источника и пункта назначения транспортного уровня.

Для создания расширенного нумерованного списка доступа используется команда со следующим форматом (за исключением протоколов **icmp** и **igrp**):

access-list *номер-списка* {**permit | deny**} *протокол источник* [*шаблон-источника*] [*оператор порт* [*порт*]] *получатель* [*шаблон-получателя*] [*оператор порт* [*порт*]] [**established**] [**log**],

где *номер-списка* — Номер списка управления доступом. Представляет собой десятичное целое число от 100 до 199 (для расширенных IP-списков).

deny — отказ в доступе, если условие выполнено;

permit — разрешение доступа, если условие выполнено;

протокол — **и**спользуемый протокол: имя протокола (**eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **tcp**, **udp**) или число, которое представляет собой номер протокола в соответствии с RFC 1700 и может быть целым числом в диапазоне 1—255. Использование ключевого слова **ip** означает все IP протоколы;

источник, получатель — IP-адрес источника/получателя пакета, ключевое слово **host** с последующим IP-адресом (конкретный хост, шаблон не указывается и равен 0.0.0.0), либо ключевое слово **any** (любой IP-адрес);

шаблон-источника, шаблон-получателя — шаблон маски, применяемый к IP-адресу источника/получателя (32-битная величина в точечно-десятичном формате, состоящем из четырех частей). Установленные в единицу биты шаблона показывают, что соответствующие биты IP-адреса источника игнорируются при проверке на соответствие адресов;

оператор — условие, накладываемое на номера портов источника/получателя (используется только для протоколов UDP и TCP). Принимает одно из следующих значений: **lt** (строго меньше), **gt** (строго больше), **eq** (равно), **neq** (не равно), **range** (диапазон включительно). После оператора следует номер порта (или два номера порта в случае оператора **range**), к которому этот оператор применяется;

порт — номер или идентификатор порта, следующий за *оператором* (используется только для протоколов UDP и TCP). В качестве идентификатора порта для TCP используются следующие ключевые слова: **bgp**, **ftp**, **pop3**, **smtp**, **telnet**, **www** и др. Для UDP: **rip**, **snmp**. **snmptrap**. **tftp**, **who** и др;

established — определяет сегменты TCP, передаваемые в состоянии установленного соединения (только для протокола TCP). Это значит, что данному критерию отбора будут соответствовать только TCP сегменты с установленными флагами ACK или RST;

log — установка ключевого слова **log** вызывает регистрацию информационного сообщения о результатах анализа пакета в системном журнале (*logging message*).

Соответствие конкретного IP-адреса критерию отбора определяется путем выполнения операции сравнения заданных шаблоном бит конкретного IP-адреса и адреса директивы (операция *маскирования по шаблону, wildcard masking)*. Например, директиве с адресом 172.30.16.0 с шаблоном 0.0.15.255 соответствует диапазон адресов 172.30.16.0 — 172.30.31.255.

Для протокола **icmp** команда создания расширенного нумерованного списка доступа имеет формат:

access-list *номер-списка* {**permit | deny**} **icmp** *источник* [*шаблон-источника*] *получатель* [*шаблон-получателя*] [*icmp-type* [*icmp-code*] | *icmp-message*]] [**log**],

где *icmp-type* — тип icmp-сообщения (число от 0 до 255);

icmp-code — код icmp-сообщения (число от 0 до 255);

icmp-message — Идентификатор icmp-сообщения, определяющий тип сообщения или тип сообщения плюс его код (**echo**, **echo-reply**, **host-unknown**, **host-unreachable**, **net-unreachable**, **network-unknown**, **traceroute**, **unreachable** и др.).

Для протокола **igmp** команда создания расширенного нумерованного списка доступа имеет формат:

access-list *номер-списка* {**permit | deny**} **igmp** *источник* [*шаблон-источника*] *получатель* [*шаблон-получателя*] [*igmp-type*] **[log],**

где *igmp-type* — тип icmp-сообщения (число от 0 до 15 или один из идентификаторов: **dvmrp**, **host-query**, **host-report**, **pim**, **trace**).

Все списки доступа неявно имеют в конце оператор **deny**. Это означает, что, как уже было сказано ранее любой, пакет, который не удовлетворяет критериям фильтрации одной из строк списка доступа, запрещается.

Чтобы применить список доступа для фильтрации дейтаграмм, проходящих через определенный интерфейс, для интерфейса используется команда:

ip access-group {*номер-списка-доступа* | *имя-списка-доступа*} {**in | out**}

Ключевое слово **in** или **out** определяет, будет ли список применяться к входящим или исходящим дейтаграммам соответственно. Входящими считаются дейтаграммы, поступающие к интерфейсу из сети. Исходящие дейтаграммы движутся в обратном направлении.

Анализ структуры списков доступа позволяет выделить следующие элементы для мутаций в правиле:

– тип правила: отказ или разрешение доступа;

– протокол;

– источник дейтаграммы с шаблоном;

— получатель дейтаграммы с шаблоном;

– диапазон портов (только для протоколов UDP и TCP);

— состояние установленного соединения (только для протокола TCP);

– тип icmp-сообщения;

– код icmp-сообщения;

– тип igmp-сообщения.

Кроме того, в списках доступа значим порядок следования правил и интерфейс привязки правила.

Исходя из вышесказанного, можно определить следующие мутационные операторы:

а) замена типа правила (с отказом на разрешение и наоборот);

б) замена типа протокола с добавлением при необходимости случайных дополнительных параметров правила (например, при переходе с протокола TCP на ICMP вместо диапазона портов задаются случайные тип и код сообщения);

в) изменение источника/получателя дейтаграммы:

— замена шаблона маски с увеличением и уменьшением сети;

— замена адреса сети на другой;

— замена сети на конкретный узел в пределах сети;

— замена сети на конкретный узел за границами сети;

— замена узла на сеть, включающую этот узел;

— замена узла на сеть, не включающую узел;

— замена сети/узла на все узлы (any);

— замена всех узлов (any) на сеть/узел;

г) изменение диапазона портов:

— замена условия на другое;

— смена порта в условии;

— расширение диапазона портов;

— сужение диапазона портов;

— замена диапазона на конкретный порт, попадающий и не попадающий в диапазон;

— смена диапазона портов с пересечением с оригинальным диапазоном (сдвиг диапазона вверх или вниз);

— смена диапазона портов без пересечения с оригинальным диапазоном;

д) установка и снятие состояния установленного соединения (для протокола TCP);

е) замена типа icmp-сообщения;

ж) замена кода icmp-сообщения;

и) замена типа igmp-сообщения;

к) добавление в случайное место списка доступа нового правила;

л) изменение порядка следования правил в списке доступа;

м) перенос правил на другой интерфейс и с входа на выход;

н) удаление правила из списка;

о) добавление в конец списка правила разрешающего прохождение любых дейтаграмм.

После внесения небольшого количества мутаций полученные списки доступа должны подвергаться проверке существующими тестами. Успешное прохождения тестов означает их ошибочность или неполноту.

Предложенный в данной работе мутационный анализ позволит произвести проверку качества тестов межсетевого экрана на соответствие его настроек требованиям политик безопасности. Повышение качества тестов позволит устранить трудно обнаруживаемые обычным образом ошибки в списках доступа и таким образом повысить общий уровень безопасности системы.

Необходимо отметить, что выполнение мутаций «вручную» является весьма трудоемкой задачей. По этой причине необходимо создание специального программного обеспечения для поддержки мутационного анализа.

Примечания

[1] Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации / Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.

[2] *Budd T., DeMillo R., Lipton R., Sayward F.* The design of a prototype mutation system for program testing // Proceedings of the National Computer Conference. — 1978. — P. 623—627; *Alexander R. T., Bieman J. M., Ghosh S. and Ji B.* Mutation of Java Objects // In Proceedings of ISSRE. — 2002. — P. 341—351; *Bradbury J. S., Cordy J. R. and Dingel J.* Mutation Operators for Concurrent Java (J2SE 5.0) // Mutation Analysis. — 2006. — P. 11—11; *Jia Y., Harman M.* An Analysis and Survey of the Development of Mutation Testing // IEEE T SOFTWARE ENG. — Vol. 7 — № 5. — P 649—678; *Ma Yu-Seung, Offutt J. and Kwon Y. R.* MuJava: An Automated Class Mutation System // AST '06 Proceedings of the 2006 international workshop on Automation of software test. — P. 78—84; *Offutt A. J.* A Practical System for Mutation Testing: Help for the Common Programmer // Proceedings., International. — P. 824—830.

[3] *Ховард М., Лебланк Д.* Защищенный код. — 2-е изд., испр. — М. : Русская Редакция, 2004. — 704 с.; *Shahriar H., Zulkernine M.* Mutation-based Testing of Buffer Overflow Vulnerabilities" // Proceedings of the Second International Workshop on Security in Software Engineering (IWSSE 2008), 2008. — P. 979—984.

[4] *Xie T., Martin E.* A Fault Model and Mutation Testing of Access Control Policies // WWW '07 Proceedings of the 16th international conference on World Wide Web. — P. 667—676.

[5] *Mouelhi T., Traon, Y. L. and Baudry B.* Mutation analysis for security tests qualification // Mutation'07 : Industrial Conference Practice and Research Techniques. — P. 233—242.

[6] *Mouelhi T., Fleurey F. and Baudry B.* A Generic Metamodel For Security Policies Mutation // ICSTW '08 Proceedings of the 2008 IEEE International Conference on Software Testing Verification and Validation Workshop. — P. 278—286.

[7] *Амато, В.* Основы организации сетей Cisco. — Испр. изд. — Т. 2. — М. : Вильяме, 2004. — 464 с.

ДИК Дмитрий Иванович, кандидат технических наук, доцент кафедры «Безопасность информационных и автоматизированных систем» Курганского государственного университета. E-mail: ddi@kgsu.ru

DIK Dmitry Ivanovich, Candidate of Engineering Sciences, Associate Professor of the Chair «Security of Information and Automation Systems», Kurgan State University. E-mail: ddi@kgsu.ru

УДК 004.891.3:004.942 + 004.7.056
ББК 3973-018.2

А. Р. Зайникаев, А. А. Муратов, Н. И. Синадский

Количественная оценка защищенности объектов информационно-телекоммуникационных систем и сетей на основе формирования графов атак с применением перечней уязвимостей и карты сетевой топологии

A. R. Zaynikaev, A. A. Muratov, N. I. Sinadskiy

Informational-telecommunicational systems and networks objects security's quantitative estimate on the basis of forming graphs of attacks using vulnerabilities lists and network topology map

Статья описывает новый метод автоматизированной оценки защищенности объектов компьютерных систем с учетом аспектов конфиденциальности, целостности и доступности. Метод позволяет проводить количественную оценку защищенности по автоматически собираемым данным без привлечения экспертов по сетевой безопасности. Оценка защищенности проводится по результатам выявления уязвимостей сканерами безопасности с учетом данных о структуре сети. В алгоритме оценки применяются нейронные сети, сформированные по графу возможных атак на узлы.

***Ключевые слова**: оценка защищенности, метрики защищенности, уровень защищенности, сетевая инфраструктура, уязвимости, граф атак.*

The paper describes a new method of a computer system objects security's automated estimate including confidentiality, integrity, and availability aspects. The method allows to conduct a quantitative estimate of a security using automatically collected data without network security experts. The security estimate is conducted by vulnerability detection results using security scanners with data about a network structure. Neural networks formed by a graph of possible attacks on hosts are used in an estimate algorithm.

***Keywords**: security estimate, security metrics, security level, network infrastructure, vulnerabilities, graph of attacks.*

Введение

Возрастающая сложность современных информационно-телекоммуникационных систем и сетей (ИТСиС), увеличивающееся количество объектов таких сетей, подключаемых к сети Интернет, представляют значительную угрозу для их безопасности при воздействии изощренных компьютерных атак. С целью предупреждения компьютерных атак предусматривается процедура аудита информационной безопасности, проводимая, в частности, с использованием программных средств — сканеров безопасности. Аудит безопасности позволяет выявить уязвимости объектов ИТСиС, способствующие осуществлению компьютерных атак. Сканеры безопасности предоставляют перечни обнаруженных ими уязвимостей на отдельном объекте ИТСиС. Одной из задач, решаемых в процессе аудита безопасности, является оценка защищенности ИТСиС в целом.

Ряд исследований в данной области посвящен получению различных способов оценки защищенности компьютерных систем. В настоящей статье предлагается метод получения количественной оценки защищенности, построенной на основе качественной оценки защищенности отдельных объектов ИТСиС с учетом сетевой инфраструктуры.

В работе используется *общая система оценки уязвимостей* (Common Vulnerability Scoring System, CVSS) [1]. Система CVSS предназначена для определения общей оценки и классификации существующих и новых уязвимостей по шкале критичности от 0 до 10. Другими словами, эта система позволяет классифицировать известные и новые уязвимости согласно риску, который представляют эти уязвимости для ИТСиС.

В случае значительного количества уязвимостей, обнаруженных сканерами безопасности на многочисленных объектах ИТСиС, возникает задача ранжирования таких объектов по степени их критичности с точки зрения воздействия на ИТСиС в целом. Устранение каждой из уязвимостей требует значительных трудозатрат системных администраторов и администраторов безопасности. Для оптимизации усилий необходимо установить, какие объекты ИТСиС находятся под максимальной угрозой, и какие именно аспекты защищенности (конфиденциальность, целостность и доступность) являются наиболее уязвимыми. Несмотря на наличие программного обеспечения, позволяющего ускорить и частично автоматизировать анализ защищенности ИТСиС, решающую роль в определении угрозы для отдельных узлов имеет эксперт, принимающий решение на основе своего опыта. В то же время систем, позволяющих решить указанную задачу на основе автоматически собираемых данных без участия квалифицированного оператора, на данный момент не известно.

Алгоритм формирования количественной оценки защищенности ИТСиС

В качестве основы для разработки алгоритма количественной оценки защищенности были рассмотрены работы И. В. Котенко и М. В. Степашкина [2], в которых подробно описано получение оценки безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности. Предложенный в [2] подход был усовершенствован с целью формирования количественной оценки защищенности на базе качественной оценки.

Входными данными для разработанного алгоритма являются отчет сканера безопасности Nessus и данные о сетевом взаимодействии. Данные о структуре сети формируются с помощью разработанной в УрФУ программы построения карты сети Nemo.

Как уже отмечалось выше, обобщенная оценка критичности уязвимости определяется с помощью системы CVSS. Размер ущерба, вызванный успешной реализацией атакующего действия, можно получить, зная критичность уязвимости и критичность сетевого узла. Для определения степени возможности реализации угрозы следует воспользоваться индексом CVSS «сложность доступа» из множества базовых индексов CVSS, задаваемых для каждого атакующего действия. Из сложности доступа можно получить степень возможности реализации угрозы. Далее из размера ущерба и степени возможности реализации угрозы может быть получен уровень риска, зная который, можно вычислить уровни защищенности узла по аспектам конфиденциальности, целостности и доступности, позволяющие в итоге получить уровень защищенности узла. Зная уровень защищенности каждого узла, можно получить уровень защищенности ИТСиС, то есть качественную оценку.

Полученная оценка уровня риска может интерпретироваться следующим образом. Уровень A — связанные с риском действия (например, внедрение новых средств защиты информации или устранение уязвимостей) должны быть выполнены немедленно и в обязательном порядке. Уровень B — связанные с риском действия должны быть предприняты. Уровень C — требуется мониторинг ситуации (но непосредственных мер по противодействию угрозе принимать, возможно, не нужно). Уровень D — никаких действий в данный момент предпринимать не требуется.

Исходя из полученных качественных оценок уровня риска для всех угроз, можно определить уровень защищенности каждого узла по каждому из векторов «конфиденциальность», «целостность», «доступность» следующим образом:

$$SecurityLevel(h,f)=\begin{cases} Green,\ \text{если}\ \forall i\in[1,N_{T_h}] \\ \qquad RiskLevel(T_{h_i},f)=D, \\ Yellow,\ \text{если}\ \exists J\subset[1,N_{T_h}]: \\ \qquad \forall j\in J\ \ RiskLevel(T_{h_j},f)=C, \\ \qquad u\ \ \forall i\notin J\ \ RiskLevel(T_{h_i},f)=D, \\ Orange,\ \text{если}\ \exists J\subset[1,N_{T_h}]: \\ \qquad \forall j\in J\ \ RiskLevel(T_{h_j},f)=B, \\ \qquad u\ \ \forall i\notin J\ \ RiskLevel(T_{h_i},f)=D \\ \qquad \text{или}\ \ RiskLevel(T_{h_i},f)=C, \\ Red,\ \exists i\in[1,N_{T_h}]\ \ RiskLevel(T_{h_i},f)=A, \end{cases}$$

где h — узел,
параметр f может иметь три значения, а именно: конфиденциальность (Confidentiality), целостность (Integrity) и доступность (Availability),
N_{T_h} — количество всех уязвимостей для рассматриваемого узла,
T_{h_i} — какая-либо уязвимость для рассматриваемого узла,
A > B > C > D.

Определим уровень защищенности каждого узла следующим образом:

$$SecurityLevel\ (h) = MostDangerous\ \{SecurityLevel\ (h, Confidentiality), SecurityLevel\ (h, Integrity), SecurityLevel\ (h, Availability)\},$$

где операция «*MostDangerous*» означает выбор самого наихудшего варианта.

Введем параметр *NCN (h)* — Number of Connected Nodes — обозначающий количество связанных узлов с данным узлом h.

Если у заданного узла параметр $NCN\ (h) \geq 2$, то есть данный узел соединен с двумя или более узлами, а значит, он может распространить угрозу, то будем полагать понижение уровня защищенности данного узла на один пункт. Естественно, если уровень защищенности уже является наихудшим, то не обязательно понижать его на единицу. Другими словами, необходимо сделать одно из следующих переопределений уровня защищенности заданного узла:

$$\text{если } NCN\ (h) \geq 2, \text{ то}:$$
$$SecurityLevel\ (h) = \begin{cases} Yellow, \text{ если } SecurityLevel\ (h) = Green, \\ Orange, \text{ если } SecurityLevel\ (h) = Yellow, \\ Red, \text{ если } SecurityLevel\ (h) = Orange, \\ Red, \text{ если } SecurityLevel\ (h) = Red. \end{cases}$$

Пользуясь определенным выше уровнем защищенности каждого узла, определим уровень защищенности анализируемой ИТСиС следующим образом:

$$SecurityLevel = \begin{cases} Green, \text{ если } \forall i \in [1, N_h]\ SecurityLevel(h_i) = Green, \\ Yellow, \text{ если } \exists J \subset [1, N_h]: \\ \quad \forall j \in J\ SecurityLevel(h_j) = Yellow, \\ \quad u\ \forall i \notin J\ SecurityLevel(h_i) = Green, \\ Orange, \text{ если } \exists J \subset [1, N_h]: \\ \quad \forall j \in J\ SecurityLevel(h_i) = Orange, \\ \quad u\ \forall i \notin J\ SecurityLevel(h_i) = Green \text{ или} \\ \quad SecurityLevel(h_i) = Yellow, \\ Red, \text{ если } \exists i \in [1, N_h]\ SecurityLevel(h_i) = Red, \end{cases}$$

где N_h — *количество* всех узлов в сети,
J — множество (набор) каких-либо индексов.

Таким образом, получена качественная оценка защищенности ИТСиС на основе качественных методик анализа рисков. Теперь необходимо осуществить переход от полученной качественной оценки к количественной оценке защищенности ИТСиС.

Введем следующие обозначения:

- *NumberScore* — количественная оценка защищенности ИТСиС;
- *NumberRed* — количество объектов ИТСиС, уровень защищенности которых равен Red, то есть:

$$NumberRed = k, \text{ если можно упорядочить узлы так, что } \forall i \in [1, k]\ SecurityLevel(h_i) = Red, \text{ и } \forall i > k\ SecurityLevel(h_i) \neq Red;$$

- аналогично *NumberOrange, NumberYellow и NumberGreen* — количество объектов ИТСиС, уровень защищенности которых равен Orange, Yellow и Green;
- *NumberAll* — количество всех компьютеров в сети, то есть:

NumberAll = NumberRed + NumberOrange + + NumberYellow + NumberGreen.

Для осуществления перехода от качественной оценки к количественной необходимо произвести следующие действия. Определим границы количественной оценки защищенности ИТСиС в зависимости от качественной оценки следующим образом:

$$NumberScore = 1, \text{ если } SecurityLevel = Green,$$
$$NumberScore \in \begin{cases} \left[\frac{2}{3}, 1\right), \text{ если } SecurityLevel = Yellow, \\ \left[\frac{1}{3}, \frac{2}{3}\right), \text{ если } SecurityLevel = Orange, \\ \left[0, \frac{1}{3}\right), \text{ если } SecurityLevel = Red. \end{cases}$$

Требуется разделить отрезок [0, 1] на три равные части, которые соответствуют качественным оценкам защищенности ИТСиС: Red, Orange и Yellow, а правая граница данного отрезка соответствует уровню Green.

Введем весовые коэффициенты для всех качественных оценок защищенности следующим образом *WeightRed* = 0; *WeightOrange* = = 1/3; *WeightYellow* = 2/3; *WeightGreen* = 1.

Обосновать выбор именно таких весовых коэффициентов можно следующим образом. Когда уровень защищенности сети равен Red, то значение количественной оценки близко к нулю, поэтому и весовой коэффициент для этого уровня нулевой. Соответственно, когда уровень равен Green, то значение равно единице, что является наибольшим уровнем. Аналогичным образом можно пояснить выбор весовых коэффициентов для уровней Yellow и Orange.

Рассчитаем среднюю оценку защищенности сети AverageScore. Для этого переопределим некоторые величины:

$NumberRed = Number_0$, $NumberOrange = Number_1$,
$NumberYellow = Number_2$, $NumberGreen = Number_3$;
$WeightRed = Weight_0$, $WeightOrange = Weight_1$,
$WeightYellow = Weight_2$, $WeightGreen = Weight_3$.

Тогда формула для средней оценки будет иметь следующий вид:

$$AverageScore = \frac{\sum_{i=0}^{3} Number_i \cdot Weight_i}{NumberAll}.$$

Теперь можно осуществить переход:

1. На уровне защищенности сети, равном Red, Orange или Yellow, следует вычислить среднюю оценку защищенности;
2. Полученное значение необходимо умножить на длину промежутка, то есть на 1/3, для того, чтобы не выйти за его рамки;
3. Полученный результат требуется прибавить к левой границе промежутка, чтобы полученная оценка попала в соответствующий промежуток.

Обозначим левую границу промежутка через *Left*. Ясно, что:

$$Left = \begin{cases} 0, & если \quad SecurityLevel = Red, \\ \frac{1}{3}, & если \quad SecurityLevel = Orange, \\ \frac{2}{3}, & если \quad SecurityLevel = Yellow. \end{cases}$$

Общая формула для перехода от качественной оценки защищенности ИТСиС (равной Red, Orange или Yellow) к количественной будет выглядеть следующим образом:

$$NumberScore(Left) = Left + \frac{1}{3} \cdot AverageScore.$$

Как видно из данной формулы, количественная оценка зависит от левой границы промежутка, который определен выше через качественную оценку, следовательно, эта формула действительно является переходом от качественной оценки к количественной.

Итак, перейдем от качественной оценки к количественной по следующему правилу:

- если качественная оценка *SecurityLevel* = = *Green*, то количественная оценка *NumberScore* = 1;
- если качественная оценка *SecurityLevel* = = *Yellow*, то количественная оценка *NumberScore = NumberScore (2/3);*
- если качественная оценка *SecurityLevel* = = *Orange*, то количественная оценка *NumberScore = NumberScore (1/3);*
- если качественная оценка *SecurityLevel* = = *Red*, то количественная оценка *NumberScore = NumberScore (0).*

Таким образом, получена количественная оценка защищенности ИТСиС.

Оценка уязвимости объектов ИТСиС предварительно обученной нейронной сетью

Для решения задачи автоматизации ранжирования объектов ИТСиС по степени их критичности были применены нейронные сети, генерируемые на основе графа возможных атак на узлы информационной сети, в которых весовые коэффициенты синапсов и аксонов нейронов задаются на основе заранее подобранных констант для различных значений метрик по системе оценки уязвимостей CVSS. Выходной сигнал каждого нейрона соответствует уровню компрометации соответствующего ему узла сети по одной из компонент вектора защищенности: конфиденциальности, целостности или доступности. Определение весовых коэффициентов входов нейронов на основе оценок уязвимостей, содержащихся в базах оценок уязвимостей в метриках CVSS, позволяет с высокой точностью учитывать влияние на защищенность узла всех обнаруженных на нем уязвимостей без привлечения эксперта. Построение нейронной сети на основе графа атак информационной сети позволяет полностью учесть при оценке защищенности особенности топологии ИТСиС.

Новизна предлагаемого метода заключается в методике предварительного обучения

системы оценки защищенности на основе экспертных оценок безопасности для отдельных узлов ИТСиС в базе обучающих примеров. В ходе обучения системы определяются константы, задающие степень влияния на оценку защищенности значений, которые могут принимать метрики CVSS. В разработанном решении константы генерируются для каждого из возможных значений метрик системы CVSS Confidentiality Impact, Integrity Impact и Availability Impact, определяющих влияние уязвимости на конфиденциальность, целостность и доступность данных на узле, а также Confidentiality Requirement, Integrity Requirement и Availability Requirement, описывающих требования к конфиденциальности, целостности и доступности данных. Кроме того, отдельные константы применяются для определения пологости нормирующих функций нейронов. Обучение нейронных сетей, построенных на основе тестовых примеров, позволяет добиться совпадения оценок, выдаваемых системой, с экспертными оценками защищенности, и, таким образом, обобщить практический опыт экспертов. Достаточно разнообразная база обучающих примеров обеспечит высокий уровень соответствия оценок системы экспертным оценкам, и, после однократного обучения системы, возможно ее применение для автоматизации работы экспертов. В случае изменения ситуации и потери точности оценок защищенности система может быть переучена с учетом новых конфигураций ИТСиС и уязвимостей, и, таким образом, будет восстановлена корректность оценок.

В качестве исходных данных для построения нейронной сети используются результаты сканирования информационной сети программой Nessus, а также данные о топологии сети. Генерация нейронной сети начинается с построения графа возможных атак на узлы (*node-predictive graph*) [3]. Вершинами такого графа являются наборы равнозначных с точки зрения уязвимости узлов сети, объединенных в группы, а ребрами — наборы уязвимостей, позволяющих провести атаку из узлов вершины графа на каждый узел, принадлежащий другой вершине.

Генерация графа начинается с вершины злоумышленника, которая добавляется как первый элемент в очередь поиска вершин. Для каждой вершины в очереди выявляются узлы, которые могут быть непосредственно атакованы из узлов этой вершины [3]. Происходит динамическое связывание обнаруженных уязвимых сетевых узлов. Динамическое связывание объединяет узлы в группы, если они могут быть атакованы одинаково, то есть при атаке с одного и того же узла можно получить одинаковый эффект. После этого узлы из группы добавляются в конец очереди, и поиск продолжается до исчерпания очереди. Общая сложность алгоритма не превосходит $O(N^3)$, где N — число узлов.

Вершины построенного графа атак разделяются на уровни вложенности, уровень вложенности вершины равен длине кратчайшего пути в графе от нее до начальной. При анализе защищенности по аспектам конфиденциальности, целостности или доступности узла применяется отдельный набор коэффициентов, и каждый из этих аспектов анализируется отдельно. Для анализа строится многослойная нейронная сеть с числом слоев, равным числу уровней вложенности в графе, и числом нейронов в каждом слое, равным количеству узлов в вершинах с уровнем вложенности, равным номеру слоя. Узлу сети в каждой вершине в соответствие ставится нейрон, представляющий из себя адаптивный взвешенный сумматор. Весовые коэффициенты входов каждого нейрона вычисляются по формуле

$$f(x) = \frac{K_R}{1+e^{-\alpha_{Rs}\sum_l K_l N_l}}.$$

В приведенной формуле K_R — коэффициент требований к защищенности по выбранному аспекту. Требования к защищенности определяются в метриках системы CVSS как «низкие», «средние» или «высокие» по таблице соответствия требований к защищенности по отношению к выбранному аспекту информационной безопасности и масштабов негативных эффектов, возникающих в случае нарушения защищенности, и могут быть определены достаточно точно без привлечения эксперта. Значение N_l — количество уязвимостей на узле с уровнем компрометации l анализируемого аспекта безопасности, то есть с полной, частичной компрометацией узла, и не компрометирующих узел. Константа K_l — коэффициент для оцениваемого аспекта безопасности и уровня компрометации узла, достигаемого уязвимостью. Коэффициент α_{Rs} задает пологость нормирующей функции для оцениваемого аспекта защищенности. При этом в расчете коэффициента используются только уязвимости, доступные для применения из узла сети, соответствующего связанному с текущим нейроном по рассматриваемому синапсу. Построенная нейронная сеть активируется подачей сигнала из нулевого слоя, соответствующего атакующим узлам.

Выходной сигнал каждого нейрона нормируется логистической функцией

$$f(x) = \frac{1}{1 + e^{-\alpha_{Ra} x}},$$

где α_{Ra} — коэффициент пологости нормирующей функции для аспекта защищенности, и интерпретируется как уровень критичности уязвимости по предложенному аспекту защищенности.

Поскольку точность оценок, получаемых системой, в значительной степени зависит от значений константных коэффициентов, применяемых в расчете весовых коэффициентов входов нейронов, то ключевым моментом в подготовке системы к работе является их определение. Получение коэффициентов значений оценок по метрикам CVSS и пологости нормирующих функций производится с помощью генетического алгоритма. В качестве генов используются искомые коэффициенты, хромосомы составляются из набора этих генов. Гены хромосом стартовой популяции определяются с помощью генератора случайных чисел. Обучение проходит по классическому генетическому алгоритму, включающему этапы скрещивания и мутации хромосом. Оценка приспособленности проводится по сумме квадратов погрешностей выходных сигналов и ожидаемых значений для всех нейронов сети и всех тестовых сетей. При этом если выходные сигналы всех нейронов во всех тестах не отличаются от эталонных более чем на заданное значение точности δ, то обучение считается завершенным, и значения коэффициентов полученного генома закрепляются как актуальные константы.

Селекция хромосом для создания следующей популяции проводится турнирным методом со случайным выбором, при котором из родительского набора хромосом случайным образом выбираются группы по три хромосомы, а затем для репродукции в каждой группе отбираются хромосомы с максимальной оценкой приспособленности. Для создания следующего поколения из полученных в результате турнира хромосом попарно выбираются случайные хромосомы, между которыми проводится скрещивание и мутация, до полного заполнения новой популяции. Для минимизации влияния положения генов в хромосоме при скрещивании выбираются две позиции в хромосоме, гены в которых выбираются в потомка из первой родительской хромосомы, а извне этих позиций — из второй. После скрещивания с вероятностью 20% один из генов меняется случайным образом. Генетический алгоритм выполняется до достижения требуемой точности значений выходных сигналов нейронов δ, либо пока не будет достигнуто предельное число популяций P_{max}, и в этом случае генетический алгоритм перезапускается с вновь сгенерированной случайной начальной популяцией.

Заключение

Результатом работы стал прототип программного комплекса, проводящий автоматическую оценку уровня защищенности каждого объекта ИТСиС с учетом топологии сети. Разработанный прототип позволяет выполнять следующие действия: загружать карты топологии ИТСиС, описания узлов и уязвимостей информационной сети в формате сканера безопасности Nessus; проводить расчет оценок защищенности узлов по аспектам конфиденциальности, целостности и доступности и представлять их в легко воспринимаемом графическом виде, проводить дополнительное уточнение расчетных коэффициентов на новых обучающих примерах информационных сетей.

Литература

1. *Mell, Peter* A Complete Guide to the Common Vulnerability Scoring System Version 2.0 / Peter Mell, Karen Scarfone, Sasha Romanovsky — http://www.first.org/cvss/cvss-guide.
2. Котенко, И. В. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности / И. В. Котенко, М. В. Степашкин, В. С. Богданов // Труды СПИИРАН. — Вып. 3. — Т. 2. — СПб. : Наука, 2006.
3. Lippmann, R. P. Evaluating and Strengthening Enterprise Network Security Using Attack Graphs / R. P. Lippmann, K. W. Ingols, C. Scott, K. Piwowarski, K. J. Kratkiewicz, M. Artz, R. K. Cunningham. 2005.
4. Sheyner, O. Automated Generation and Analysis of Attack Graphs / O. Sheyner et al. // 2002 IEEE Symposium on Security and Privacy, Oakland, CA, 2002.

ЗАЙНИКАЕВ Алексей Русланович, аспирант ФГАОУ ВПО Уральский федеральный университет имени первого Президента России Б. Н. Ельцина.
E-mail : archlich@list.ru

ZAYNIKAEV Ruslanovich Alex, a graduate student FGAOU VPO Southern Federal University of the first Russian President Boris Yeltsin.
E-mail : archlich@list.ru

МУРАТОВ Алексей Александрович, аспирант, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина.
E-mail aamuratov@gmail.com

MURATOV Alexey, a graduate student FGAOU VPO Southern Federal University of the first Russian President Boris Yeltsin.

СИНАДСКИЙ Николай Игоревич, к. т. н., доцент.

SINADSKY Nicholas I., Cand., Associate Professor.

УДК 534.83:53.08 + 534.831 + 628.517.001.2
ББК В32

А. А. Копылова, К. А. Паршин

Методика расчета уровня шума в помещении путем расчета звукоизоляции помещения

A. A. Kopylova, K. A. Parshin

Technique for calculating noise levels in a room by calculating room acoustic isolation

В статье представлена разработанная методика расчета уровня шума в помещении путем расчета звукоизоляции помещения, которая не требует значительных финансовых затрат. Правомерность применения данной методики для определения уровня шума доказана с помощью теоретических знаний о звукоизоляционных свойствах помещений и элементов теории акустики, закрепленных в действующих нормативных документах.

***Ключевые слова**: уровень шума, звукоизоляция помещения, акустика, методика.*

The paper provides a low-cost technique that allows to calculate noise levels in a room by calculating room acoustic isolation. Justification of applying this technique for the purposes of noise level definition is based on theoretical knowledge about soundproofing properties of a room and some elements of acoustics theory reflected in applicable statutory regulations.

***Keywords**: Noise level, room acoustic insulation, acoustics, technique.*

Согласно [1], если ограждающая конструкция состоит из нескольких частей с различной звукоизоляцией (например, стена с окном и дверью), изоляцию воздушного шума ограждающей конструкцией R определяют по формуле

$$R = 10\lg\frac{S}{\sum_{i=1}^{n}\frac{S_i}{10^{0,1R_i}}}, \qquad (1)$$

где S_i — площадь i-й части, м^2;
R_i — изоляция воздушного шума i-й частью, дБ.

Если ограждающая конструкция состоит из двух частей с различной звукоизоляцией ($R_1 > R_2$), R определяют по формуле

$$R = R_1 - 10\lg\frac{\frac{S_1}{S_2} + 10^{0,1(R_1 - R_2)}}{1 + \frac{S_1}{S_2}}, \qquad (2)$$

1. Определяем материал и толщину ограждающих конструкций экспериментального помещения.

2. В случае наличия в ограждающих конструкциях дверных и оконных проемов, щелей, отверстий — рассчитываем их площади, а также площади ограждающих конструкций.

3. Звукоизоляцию на среднегеометрических частотах третьоктавных полос каждой из ограждающих конструкций рассчитываем графическим методом [3].

В случае наличия дверных и оконных проемов их звукоизоляция на среднегеометрических частотах третьоктавных полос определяется согласно справочным данным [3].

4. В случае наличия в ограждающих конструкциях дверных и оконных проемов, щелей, отверстий — по формулам (1—2) рассчитываем суммарную звукоизоляцию комбинированных ограждающих конструкций на всех среднегеометрических частотах третьоктавных полос.

5. Строим частотные характеристики ограждающих конструкций, подтверждая точность построения методом интерполяции.

6. Недостающие значения звукоизоляции на среднегеометрических частотах третьоктавных полос определяем графоаналитическим методом по построенным частотным характеристикам.

7. Определяем индекс звукоизоляции каждой ограждающей конструкции. Для этого рассчитываем сумму неблагоприятных отклонений частотной характеристики ограждающей конструкции от нормативной кривой категории 1 (табл. 3, рис. 4).

8. Если сумма неблагоприятных отклонений максимально приближается к 32 дБ, но не превышает эту величину, величина индекса звукоизоляции (R_w) составляет 53 дБ.

Если сумма неблагоприятных отклонений превышает 32 дБ, нормативная кривая смещается вниз на целое число децибел так, чтобы сумма неблагоприятных отклонений не превышала указанную величину.

Если сумма неблагоприятных отклонений значительно меньше 32 дБ или неблагоприятные отклонения отсутствуют, оценочная кривая смещается вверх на целое число децибел так, чтобы сумма неблагоприятных отклонений от смещенной оценочной кривой максимально приближалась к 32 дБ, но не превышала эту величину.

За величину индекса звукоизоляции принимают ординату смещенной вверх или вниз оценочной кривой в третьоктавной полосе со среднегеометрической частотой 500 Гц.

9. Из полученных значений индексов звукоизоляции каждой ограждающей конструкции выбираем наименьший. Он и будет являться индексом звукоизоляции помещения.

10. После расчета звукоизоляции экспериментального помещения определяем местоположение этого помещения относительно транспортных потоков на улицах и дорогах городов и согласно [5] определяем шумовую характеристику транспортных потоков, воздействующую на помещение.

11. Значение уровня шума в экспериментальном помещении рассчитываем как разность между значением шумовой характеристики транспортного потока и значением звукоизоляции самого помещения.

Рассмотрим пример. Помещение 1 (рис. 1) состоит из следующих конструкций:

1) внутренняя перегородка из железобетона толщиной 100 мм (размеры перегородки — 6,98×2,89 м);

2) внутренняя перегородка из кирпича толщиной 65 мм (одинарный) (размеры перегородки — 6,08×2,89 м) с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м);

3) внешняя стена из железобетонных блоков толщиной 200 мм (размеры стены — 6,98×2,89 м) с двумя деревянными окнами с двойным остеклением и воздушным промежутком (размеры окна 1 — 1,31×1,52 м, окно 2 — 1,91×1,52 м), а также с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м);

4) внутренняя перегородка из кирпича толщиной 65 мм (одинарный) (размеры перегородки — 6,08×2,89 м) с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м).

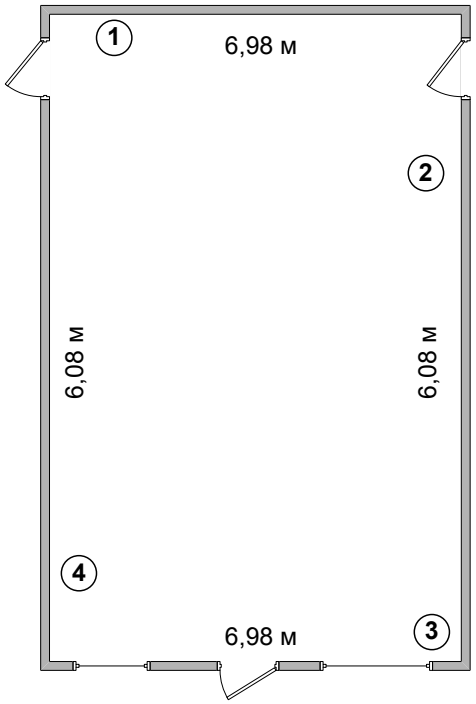


Рис. 1. Экспериментальное помещение 1

Звукоизоляцию отдельных ограждающих конструкций рассчитываем графическим методом.

1. Перегородка из железобетона (100 мм);
$f_{Вж/б}$ = 250 Гц;
$R_{Вж/б}$ = 37 дБ.

Таблица 1

Звукоизоляция перегородки из железобетона на средних частотах третьоктавных полос

Наименование показателя	Средние частоты третьоктавных полос, Гц																
	100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
Изоляция воздушного шума перегородки из железобетона *R*, дБ	37	37	37	37	37	41	42	44	46	48	50	52	53	55	56	58	60

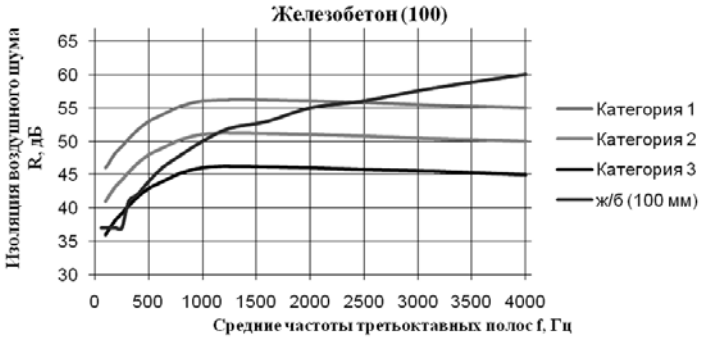


Рис. 2. Частотная характеристика изоляции воздушного шума перегородки из железобетона

Расчет индекса звукоизоляции проводится по форме табл. 2. Вносим в таблицу значения *R* оценочной кривой (категория 2) и находим неблагоприятные отклонения расчетной частотной характеристики от оценочной кривой (пункт 3). Средняя величина отклонений должна максимально приближаться к 32 дБ, но не превышать эту величину.

Определим индекс звукоизоляции внутренней перегородки из железобетона (табл. 2). Сумма неблагоприятных отклонений составила 47 дБ, что превышает требуемое значение в 32 дБ. Смещаем оценочную кривую вниз на 2 дБ и находим сумму неблагоприятных отклонений уже от смещенной оценочной кривой. На этот раз она составляет 26 дБ, что максимально приближается к 32 дБ. За величину индекса изоляции принимаем значение смещенной оценочной кривой в 1/3-октавной полосе 500 Гц, т. е. $R_{Ж/Б}$ = 46 дБ.

Таблица 2

Определение индекса звукоизоляции перегородки из железобетона

№ п/п	Параметры	Среднегеометрическая частота 1/3-октавной полосы, Гц																
		100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	Расчетная частотная характеристика *R* (железобетонная перегородка), дБ	37	37	37	37	37	41	42	44	46	48	50	52	53	55	56	58	60
2	Оценочная кривая (2 категория), дБ	41	42	42	43	44	45	47	48	49	50	51	51	51	51	51	50	50
3	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	4	5	5	6	7	4	5	4	3	2	1	—	—	—	—	—	—
4	Сумма отклонений	Σ 47>32																

Окончание табл. 2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
5	Оценочная кривая, смещенная вниз на 2 дБ	39	40	40	41	42	43	45	46	47	48	49	49	49	49	49	48	48
6	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	2	3	3	4	5	2	3	2	1	0	—	—	—	—	—	—	—
7	Сумма отклонений	Σ 26≈32																
8	Индекс изоляции воздушного шума $R_{Ж/Б}$, дБ								46									

2. Перегородка из кирпича;
$f_{Вкирп}$ = 280 Гц;
$R_{Вкирп}$ = 42 дБ.

Таблица 3

Звукоизоляция перегородки из кирпича на средних частотах третьоктавных полос

Наименование показателя	Средние частоты третьоктавных полос, Гц																
	100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
Изоляция воздушного шума кирпичной перегородки *R*, дБ	42	42	42	42	42	46	49	51	53	56	58	60	63	64	65	65	65

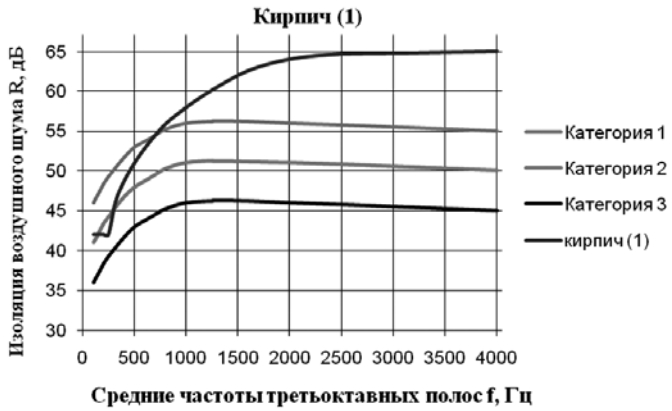


Рис. 3. Частотная характеристика изоляции воздушного шума кирпичной перегородки

Расчет индекса звукоизоляции проводится по форме табл. 4. Вносим в таблицу значения *R* оценочной кривой (категория 1) и находим неблагоприятные отклонения расчетной частотной характеристики от оценочной кривой (пункт 3). Средняя величина отклонений должна максимально приближаться к 32 дБ, но не превышать эту величину.

Определим индекс звукоизоляции внутренней перегородки из кирпича толщиной 65 мм (табл. 4). Сумма неблагоприятных отклонений составила 37 дБ, что превышает требуемое значение в 32 дБ. Смещаем оценочную кривую вниз на 1 дБ и находим сумму неблагоприятных отклонений уже от смещенной оценочной кривой. На этот раз она составляет 28 дБ, что максимально приближается к 32 дБ. За величину индекса изоляции принимаем значение смещенной оценочной кривой в 1/3-октавной полосе 500 Гц, т. е. $R_к$ = 52 дБ.

Таблица 4

Определение индекса звукоизоляции внутренней перегородки из кирпича

№ п/п	Параметры	Среднегеометрическая частота 1/3-октавной полосы, Гц																
1	Расчетная частотная характеристика *R* (внутренняя перегородка из кирпича), дБ	42	42	42	42	42	46	49	51	53	56	58	60	63	64	65	65	65
2	Оценочная кривая (1 категория), дБ	46	47	47	48	49	50	52	53	54	55	56	56	56	56	56	55	55
3	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	4	5	5	6	7	4	3	2	1	—	—	—	—	—	—	—	—
4	Сумма отклонений	Σ 37>32																
5	Оценочная кривая, смещенная вниз на 1 дБ	45	46	46	47	48	49	51	52	53	54	55	55	55	55	55	54	54
6	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	3	4	4	5	6	3	2	1	0		—	—	—	—	—	—	—
7	Сумма отклонений	Σ 28≈32																
8	Индекс изоляции воздушного шума $R_к$, дБ								52									

3. Стена из железобетона (200 мм);
$f_{Вшл}$ = 240 Гц;
$R_{Вшл}$ = 43 дБ.

Таблица 5

Звукоизоляция стены из железобетона на средних частотах третьоктавных полос

Наименование показателя	Средние частоты третьоктавных полос, Гц																
	100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
Изоляция воздушного шума стены из железобетона *R*, дБ	43	43	43	43	44	46	48	51	53	56	59	61	63	65	65	65	65

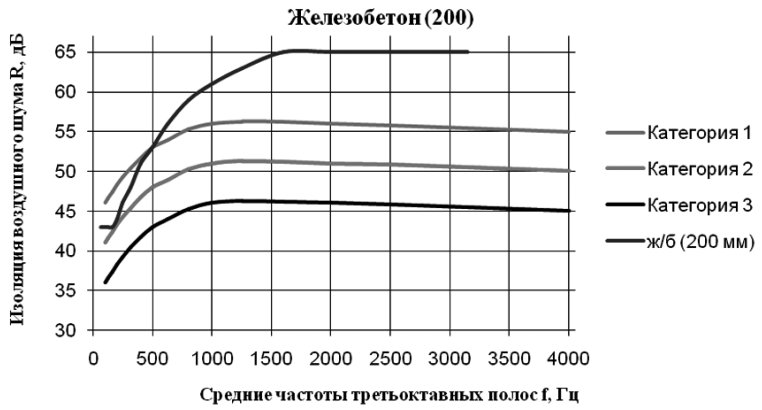


Рис. 4. Частотная характеристика изоляции воздушного шума стены из железобетона

Расчет индекса звукоизоляции проводится по форме таблицы 6. Вносим в таблицу значения *R* оценочной кривой (категория 1) и находим неблагоприятные отклонения расчетной частотной характеристики от оценочной кривой (пункт 3). Средняя величина отклонений должна максимально приближаться к 32 дБ, но не превышать эту величину.

Определим индекс звукоизоляции внешней железобетонной стены (200 мм) (табл. 6). Сумма неблагоприятных отклонений составила 32дБ, что равно требуемому значению в 32 дБ. За величину индекса изоляции принимаем значение оценочной кривой в 1/3-октавной полосе 500 Гц, т. е. $R_{Ж/Б\ (200)}$ = 53 дБ.

Таблица 6

Определение индекса звукоизоляции внешней стены из железобетонных блоков (200 мм)

№ п/п	Параметры	Среднегеометрическая частота 1/3-октавной полосы, Гц																
		100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	Расчетная частотная характеристика R (внешняя стена из железобетона), дБ	43	43	43	43	44	46	48	51	53	56	59	61	63	65	65	65	65
2	Оценочная кривая (1 категория), дБ	46	47	47	48	49	50	52	53	54	55	56	56	56	56	56	55	55
3	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	3	4	4	5	5	4	4	2	1	—	—	—	—	—	—	—	—
4	Сумма отклонений	Σ 32=32																
5	Индекс изоляции воздушного шума $R_{ж/б}$, дБ								53									

Звукоизоляцию оконных проемов и дверей берем из справочника.

Для расчета звукоизоляции ограждающих конструкций, состоящих из нескольких частей с разной звукоизоляцией, воспользуемся формулой (1).

В случае, когда ограждающая конструкция состоит из двух частей с различной звукоизоляцией ($R_1 > R_2$), R определим по формуле (2).

Рассчитываем звукоизоляцию:

1. внутренней перегородки из кирпича толщиной 65 мм (одинарный) (размеры перегородки — 6,08×2,89 м) с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м);

2. внешней стены из железобетонных блоков толщиной 200 мм (размеры стены — 6,98×2,89 м) с двумя деревянными окнами с двойным остеклением и воздушным промежутком (размеры окна 1 — 1,31×1,52 м, окно 2 — 1,91×1,52 м), а также с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м);

внутренней перегородки из кирпича толщиной 65 мм (одинарный) (размеры перегородки — 6,08×2,89 м) с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м).

Идентичность внутренних перегородок из кирпича толщиной 65 мм с дверью из пластикового стеклопакета позволяет произвести расчет только для одной из них.

Рассчитанные данные заносим в табл. 7.

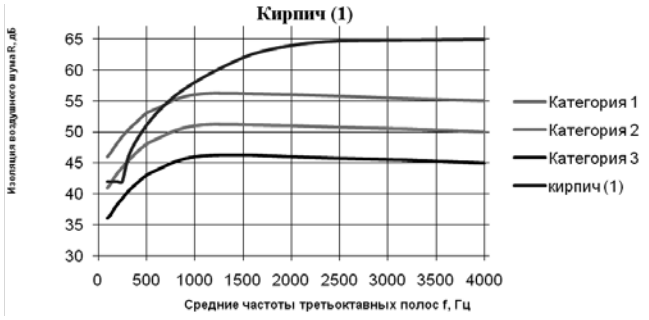
Таблица 7

Звукоизоляция ограждающих конструкций, состоящих из двух частей

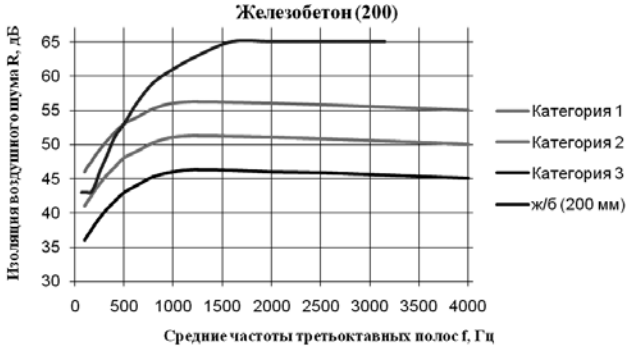
Тип	Конструкция	Звукоизоляция R (дБ) на частотах, Гц																
		100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
1. Внутренняя перегородка из кирпича с дверью из пластикового стеклопакета	Стена: Толщина — 65 мм, высота — 2,89 м, ширина — 6,08 м. Дверь: Толщина стекла — 4 мм, возд. промежуток — 12 мм, высота — 2,1 м, ширина — 0,95 м	33	32	30	27	27	28	31	34	38	43	47	49	50	51	50	49	48
2. Внешняя стена из железобетонных блоков с двумя деревянными окнами с двойным остеклением и воздушным прмежутком, а также с дверью из пластикового стеклопакета	Стена: Толщина — 200 мм, высота — 2,89 м, ширина —6,98 м. Дверь: Толщина стекла — 4 мм, возд. промежуток — 12 мм, высота — 2,1 м, ширина — 0,95 м. Окно 1: Толщина стекла — 4 мм, возд. промежуток — 57 мм, высота — 1,52 м, ширина — 1,31 м. Окно 2: Толщина стекла — 4 мм, возд. промежуток — 57 мм, высота — 1,52 м, ширина — 1,91 м.	29	29	28	27	27	28	31	34	38	42	46	48	49	49	48	45	40

Построим частотные характеристики для данных ограждающих конструкций (рис. 5).

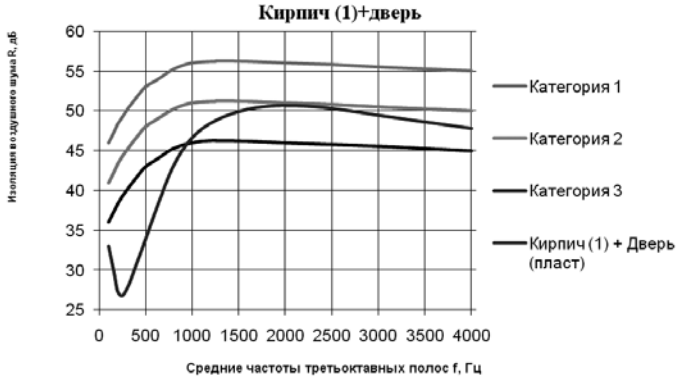
а



б



в



г

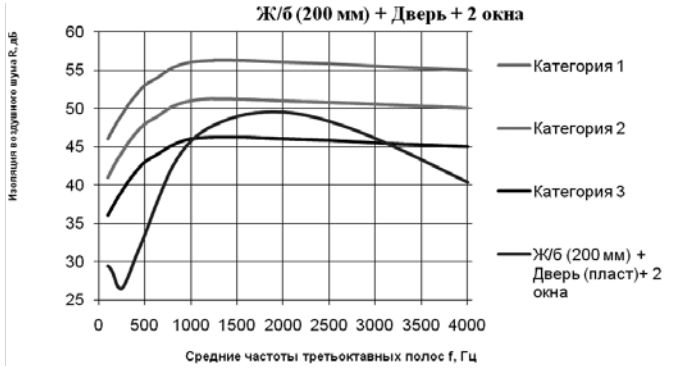


Рис. 5. Расчетные частотные характеристики: а — частотная характеристика звукоизоляции внутренней перегородки из кирпича; б — частотная характеристика звукоизоляции внешней стены из железобетонных блоков (200 мм); в — частотная характеристика звукоизоляции внутренней перегородки из кирпича толщиной 65 мм (размеры перегородки — 6,08×2,89 м) с дверью из пластикового стеклопакета; г — частотная характеристика звукоизоляции внешней стены из железобетонных блоков толщиной 200 мм с двумя деревянными окнами с двойным остеклением и воздушным промежутком, а также с дверью из пластикового стеклопакета.

Расчет индекса звукоизоляции проводится по форме табл. 8. Вносим в таблицу значения *R* оценочной кривой (категория 3) и находим неблагоприятные отклонения расчетной частотной характеристики от оценочной кривой (пункт 3). Средняя величина отклонений должна максимально приближаться к 32 дБ, но не превышать эту величину.

Определим индекс звукоизоляции внутренней перегородки из кирпича (табл. 8). Сумма неблагоприятных отклонений составила 80 дБ, что превышает требуемое значение в 32 дБ. Смещаем оценочную кривую вниз на 6 дБ и находим сумму неблагоприятных отклонений уже от смещенной оценочной кривой. На этот раз она составляет 28 дБ, что максимально приближается к 32 дБ. За величину индекса изоляции принимаем значение смещенной оценочной кривой в 1/3-октавной полосе 500 Гц, т. е. $R_{К(1)+дверь}$ = 37 дБ.

Таблица 8

Определение индекса звукоизоляции внутренней перегородки из кирпича (размеры перегородки — 6,08×2,89 м) с дверью из пластикового стеклопакета

№ п/п	Параметры	Среднегеометрическая частота 1/3-октавной полосы, Гц																
		100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
1	Расчетная частотная характеристика *R* (внутренняя перегородка из кирпича (1) с дверью), дБ	33	32	30	27	27	28	31	34	38	43	47	49	50	51	50	49	48
2	Оценочная кривая (3 категория), дБ	36	37	37	38	39	40	42	43	44	45	46	46	46	46	46	45	45
3	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	3	5	8	11	12	12	11	9	6	2	—	—	—	—	—	—	—
4	Сумма отклонений	Σ 80 > 32																
5	Оценочная кривая, смещенная вниз на 6 дБ	30	31	31	32	33	34	36	37	38	39	40	40	40	40	40	39	39
6	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	—	—	2	5	6	6	5	3	—	—	—	—	—	—	—	—	—
7	Сумма отклонений	Σ 28≈32																
8	Индекс изоляции воздушного шума $R_{К(1)+дверь}$, дБ								37									

Аналогично рассчитываем индекс звукоизоляции для внешней стены из железобетонных блоков толщиной 200 мм с двумя деревянными окнами с двойным остеклением и воздушным промежутком, а также с дверью из пластикового стеклопакета (табл. 9).

Таблица 9

Определение индекса звукоизоляции внешней стены из железобетонных блоков с двумя деревянными окнами с двойным остеклением и воздушным промежутком, а также с дверью из пластикового стеклопакета

№ п/п	Параметры	Среднегеометрическая частота 1/3-октавной полосы, Гц																
		100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
1	Расчетная частотная характеристика *R* (внешняя стена из ж/б блоков с двумя окнами и дверью), дБ	29	29	28	27	27	28	31	34	38	42	46	48	49	49	48	45	40
2	Оценочная кривая (3 категория), дБ	36	37	37	38	39	40	42	43	44	45	46	46	46	46	46	45	45
3	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	7	7	9	11	13	12	11	9	6	3	—	—	—	—	—	—	5
4	Сумма отклонений	Σ 89 > 32																
5	Оценочная кривая, смещенная вниз на 7 дБ	29	30	30	31	32	33	35	36	37	38	39	39	39	39	39	38	38
6	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	—	—	2	4	6	5	4	2	—	—	—	—	—	—	—	—	—
7	Сумма отклонений	Σ 24≈32																
8	Индекс изоляции воздушного шума $R_{Ж/Б(200)+2окна+дверь}$, дБ								36									

Таким образом, индексы звукоизоляции для данных ограждающих конструкций:

1. $R_{Ж/Б}$ = 46 дБ,
2. $R_{К(1)\ +\ дверь}$ = 37 дБ,
3. $R_{Ж/Б(200)+2окна\ +\ дверь}$ = 36 дБ,
4. $R_{К(1)\ +\ дверь}$ = 37 дБ.

Так как звукоизоляция помещения определяется по звукоизоляции ограждающей конструкции, имеющей наименьшее значение, следовательно, звукоизоляция рассматриваемого помещения равна 36 дБ.

Согласно [5] расчетные шумовые характеристики транспортных потоков на улицах и дорогах городов для условий движения транспорта в час «пик» допускается принимать по табл. 10.

Таблица 10

Шумовые характеристики транспортных потоков

Категория улиц и дорог	Число полос движения проезжей части в обоих направлениях	Шумовая характеристика транспортного потока в дБА
Скоростные дороги	6	86
	8	87
Магистральные улицы и дороги общегородского значения:		
непрерывного движения	6	84
	8	85
регулируемого	4	81
	6	82
районного значения	4	81
	6	82
дороги грузового движения	2	79
	4	81
Улицы и дороги местного значения:		
жилые улицы	2	73
	4	75
дороги промышленных и коммунально-складских районов	2	79

В связи с тем, что рассматриваемое помещение непосредственно фасадом здания (стена из железобетонных блоков) прилегает к проезжей части, которая состоит из двух полос и является дорогой местного значения, шумовая характеристика транспортного потока будет равна 73 дБ (см. табл. 10).

Так как расчетная звукоизоляция помещения составила 36 дБ, а шумовая характеристика транспортного потока принимается равной 73 дБ, то уровень шума внутри помещения составит 37 дБ.

Аналогичным образом был произведен расчет уровня шума еще в двух помещениях.

Помещение 2 (рис. 6) состоит из следующих конструкций:

1) внутренняя перегородка из гипсокартона толщиной 12,5 мм (размеры перегородки — 3,5×2,8 м) с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м);

2) внутренняя перегородка из гипсокартона толщиной 12,5 мм (размеры перегородки — 3,52×2,8 м) с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м);

3) внутренняя перегородка из гипсокартона толщиной 12,5 мм (размеры перегородки — 7,06×2,8 м) с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м);

4) внутренняя оштукатуренная кирпичная стена толщиной 250 мм (размеры стены — 4,57×2,8 м);

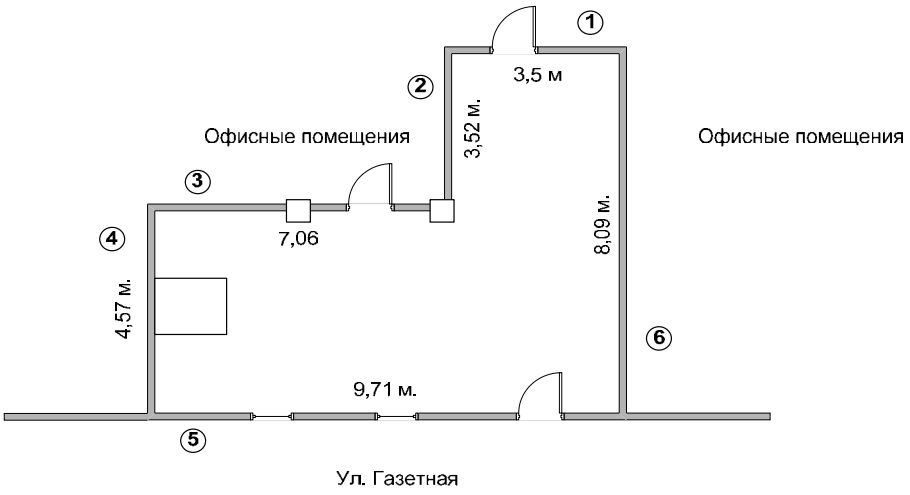


Рис. 6. Экспериментальное помещение 2

5) внешняя стена из шлакоблоков толщиной 220 мм (размеры стены — 9,71×2,8 м) с двумя окнами из двойного пластикового стеклопакета (размеры окна — 1,9×1,3 м), а также с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м);

6) внутренняя оштукатуренная кирпичная стена толщиной 250 мм (размеры стены — 8,09×2,8 м).

Расчетный уровень шума в помещении 2 равен 49 дБ.

Помещение 3 (рис. 7) состоит из следующих конструкций:

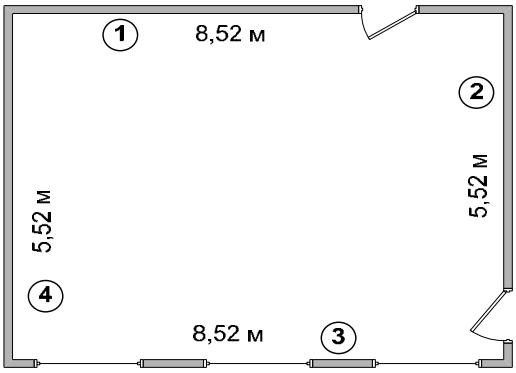


Рис. 7. Экспериментальное помещение 3

1. Внутренняя перегородка из кирпича толщиной 88 мм (полуторный) (размеры перегородки — 8,52×3,3 м) с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м);

2. Внутренняя перегородка из кирпича толщиной 88 мм (полуторный) (размеры перегородки — 5,52×3,3 м) с дверью из пластикового стеклопакета (размеры двери — 2,1×0,95 м);

3. Внешняя стена из кирпича толщиной 140 мм (двойной) (размеры стены — 8,52×3,3 м) с тремя окнами из двойного пластикового стеклопакета (размеры окон — 1,9×1,3 м);

4. Внутренняя перегородка из кирпича толщиной 65 мм (одинарный) (размеры перегородки — 5,52×3,3 м).

Расчетный уровень шума в помещении 3 равен 38 дБ.

Сравнительный анализ расчетных и измеренных значений уровня шума в экспериментальных помещениях

Полученные значения уровня шума в экспериментальных помещениях сведены в табл. 11.

Таблица 11

Сравнительный анализ расчетных и измеренных значений уровня шума в экспериментальных помещениях

№ п/п	Помещение	Шумовая характеристика транспортных потоков, дБ	Звукоизоляция, дБ	Уровень шума, дБ	
				Расчетный	Измеренный
1	Помещение 1	81	32	49	54
2	Помещение 2	73	36	37	41
3	Помещение 3	73	35	38	37,7

Как видно из табл. 11, измеренные и расчетные значения уровней шума в помещениях приблизительно равны, расхождение в значениях обусловлено погрешностью в подсчетах и измерениях.

Рассчитаем абсолютную погрешность для полученных значений по каждому из экспериментальных помещений:

$$\Delta R_1 = \frac{54-48}{54}\times 100\% = 9.26\% \ ;$$

$$\Delta R_2 = \frac{41-37}{41}\times 100\% = 9.76\% \ ;$$

$$\Delta R_1 = \frac{37.7-38}{37.7}\times 100\% = 0.8\% \ .$$

Следовательно, среднее значение погрешности будет равно:

$$\Delta \overline{R}_1 = \frac{\Delta R_1 + \Delta R_2 + \Delta R_3}{3} = 6.61\% \ .$$

Из приведенных выше вычислений видно, что в среднем рассчитанные значения уровня шума в помещениях отличаются от измеренных значений на 6,61%.

Таким образом, обязанность по контролю уровня шума на рабочих местах полностью ложится на плечи работодателя, который вынужден нести значительные финансовые затраты, привлекая сторонние специализированные организации к осуществлению различных инструментальных измерений. Разработанная методика является альтернативным вариантом определения уровня шума на рабочих местах, который не требует значительных финансовых затрат. Правомерность применения данной методики для определения уровня шума основана на

теоретических знаниях о звукоизоляционных свойствах помещений и элементов теории акустики, нормативно закрепленных в СНиП 23-03-2003 «Защита от шума», СП 23-103-2003 «Проектирование звукоизоляции ограждающих конструкций жилых и общественных зданий», а также в СНиП II-12-77 «Строительные нормы и правила. Часть II. Нормы проектирования».

Литература

1. Безопасность информационного пространства : мат-лы VIII региональной науч.-практ. конф. студентов, аспирантов и молодых ученых. — Челябинск : Издательский центр ЮУрГУ, 2009. — С. 190—192.
2. *Бузов, Г. А.* Защита от утечки информации по техническим каналам : учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. — М. : Горячая линия — Телеком, 2005. —416 с.
3. *Паршин, К. А.* Технология защиты речевой информации в помещениях : учебно-методическое пособие / К. А. Паршин, А. А. Копылова. — Екатеринбург : УрГУПС, 2010. — 88 с.
4. *СНиП 23-03-2003* «Строительные нормы и правила в Российской Федерации. Защита от шума».
5. *СНиП II-12-77* «Строительные нормы и правила. Ч. II. Нормы проектирования».
6. Федеральный закон «О коммерческой тайне» в редакции 2006 г. // Российская газета.

ПАРШИН Константин Анатольевич, доцент кафедры «Информационные технологии и защита информации», Уральский государственный университет путей сообщения. E-mail: KParshin@kt.usurt.ru

PARSHIN Konstantin Anatolievich, Associate Professor of the Chair "Information Technologies and Information Protection", Urals State University of Railway Transport; KParshin@kt.usurt.ru

КОПЫЛОВА Александра Андреевна, аспирант кафедры «Информационные технологии и защита информации», Уральский государственный университет путей сообщения. E-mail v060138@inbox.ru

KOPYLOVA Aleksandra Andreevna, Postgraduate Student of the Chair "Information Technologies and Information Protection", Urals State University of Railway Transport; e-mail v060138@inbox.ru

УДК 621.396.2:004.056
ББК 32.883

Ю. А. Михайлов

Защита информации от утечки по каналам ПЭМИн в современном мире

Yu. A. Mikhailov

Protection against information outflow via the channel of the side electromagnetic radiation and aiming in the present-day world

В статье изложены результаты краткого экскурса в историю защиты информации от утечки по техническим каналам, показана эволюция средств защиты от ПЭМИН, обоснована актуальность защиты мобильных средств обработки и хранения информации, декларированы возможности программного метода генерирования шумов, который позволит использовать аппаратные возможности мобильного устройства для его защиты.

***Ключевые слова**: защита информации, ПЭМИН, мобильные средства, генерирование шумов, программный метод.*

The article provides a brief historical review of information protection against information outflow via the channel of the side electromagnetic radiation and aiming (PEMIN) and evolution of the means of protection against PEMIN. The author substantiates the importance of protecting mobile means of information processing and storage and describes possibilities of software-based method for noise generation allowing to use hardware capabilities of a mobile device for protection purposes.

***Keywords**: Information protection, PEMIN, mobile devices, noise generation, software-based method.*

История защиты информации от утечки по техническим каналам началась в начале XX века. В то время угроза исходила от перехвата радиосигнала, во время передачи информации между радиостанциями. Однако основным способом защиты информации было предварительное шифрование и передача уже зашифрованного сообщения. Во время исследования возможностей перехвата информации по техническим каналам было выявлено побочное электромагнитное излучение (ПЭМИн), которое излучают шифровальные машины в процессе обработки информации. Исследования данного излучения доказали, что эти сигналы являются информативными и могут служить каналом утечки информации. Но в связи с невысоким уровнем используемых электронных устройств дальнейшие изучения данного эффекта были прекращены. После появления ЭВМ проблема ПЭМИн снова стала актуальной, так как уровень данного излучения от этих устройств был высокий и позволял осуществлять перехват информации на больших расстояниях. Так, в 1985 году голландский инженер Виму ван Эйку опубликовал статью «Электромагнитное излучение видеодисплейных модулей: риск перехвата?», в которой он описал, а позже и продемонстрировал возможность перехвата видеоизображения с монитора компьютера. Данное исследование стало толчком для развития средств защиты информации. В итоге основными способами защиты стали генераторы шума, которые излучали в пространство радиоволны, создающие помехи при перехвате информации, и экраны, препятствующие распространению ПЭМИн.

Эти методы стали основными и активно применялись для защиты ЭВМ и при правильном использовании снижали риск утечки информации к минимуму. Особенно эффективным является их совместное использование, когда применение экранов существенно уменьшает радиус распространения ПЭМИн, а генераторы шума создают

помехи при перехвате ПЭМИн. Однако тенденции развития современной IT-индустрии ведут к мобилизации средств обработки и хранения информации. Стационарные системы становятся менее востребованными и на смену им все чаще приходят более мобильные технические средства, позволяющие осуществлять обработку информации вне помещений. В результате повсеместного применения данных технических средств для работы с информацией невозможно предугадать, где и в какой момент времени произойдет ее утечка. А существующие способы защиты не способны обеспечить информационную безопасность в условиях использования мобильных устройств.

На данный момент защита мобильных средств обработки и хранения информации является наиболее актуальной. Особенно острым данный вопрос становится в случае использования мобильных технических средств государственными служащими и первыми лицами государства. Так, многие чиновники Государственной Думы РФ взяли на вооружение планшетные компьютеры. Учитывая незащищенность таких устройств и использование их вне зданий с высоким уровнем безопасности, можно предположить, что наиболее вероятными действиями злоумышленников будут попытки перехвата информации именно от мобильных устройств. А существующие методы защиты информации либо малопригодны, либо вовсе неприменимы для обеспечения информационной безопасности. Анализ всех существующих методов защиты показал, что на данный момент наиболее подходящим для мобильных устройств является метод экранирования. Однако использование данного метода существенно снижает эргономику мобильных средств и не гарантирует полной защиты информации из-за отсутствия возможности контролировать территорию вокруг объекта защиты. В результате требуется разработка нового метода защиты или комплекса методов, применимого для обеспечения информационной безопасности мобильных технических средств.

Одним из таких методов может служить разрабатываемый программный метод генерирования шумов, который позволит использовать аппаратные возможности мобильного устройства для его защиты. Основное описание работы данного метода изложено в статье Ю. А. Михайлова «Модель программного противодействия утечки информации по каналам ПЭМИн».

Литература

1. *Михайлов Ю. А.* Модель программного противодействия утечки информации по каналам ПЭМИн // Sibinfo. — Т. 3. — Томск, 2011.
2. http://ru.wikipedia.org/wiki/TEMPEST — статья о ПЭМИн
3. Marcus G. Kuhn «Security Limits for Compromising Emanations» University of Cambridge, CHES 2005. — P. 265—279.
4. Wim van Eck «Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?» // Computers & Security. — 1985. — № 4. — P. 269—286.

МИХАЙЛОВ Юрий Алексеевич, аспирант, Тюменский государственный университет, Институт математики, естественных наук и информационных технологий, кафедра Информационной безопасности. E-mail: windym@rambler.ru

MIKHAILOV Yury, a graduate student, Tyumen State University, Institute of Mathematics, Science and Information Technology, Department of Information Security.
E-mail: windym@rambler.ru

УДК 004:343.2/7
ББК Х408.135

И. И. Сухих

Проблемы борьбы с преступлениями в сфере компьютерной информации

I. I. Sukhikh

Problems of crime control in the field of computer information

В статье рассматривается возможность и необходимость перехода от противоречащих друг другу законов к целостному информационному кодексу. Такой шаг будет способствовать повышению уровня правовой грамотности и правосознания пользователей и достижению стабильности в инфотелекоммуникационной среде

***Ключевые слова**: безопасность в сфере компьютерной информации, компьютерные преступления, технологии информатизации и информационной безопасности.*

The paper covers the possibility and necessity of transition from conflicting laws to a holistic information code. Such step will contribute to higher levels of law knowledge and legal awareness of users and stability in information and telecommunication environment.

***Keywords**: Safety and security in the field of computer information, computer crimes, technologies of informatization and information security.*

С внедрением информационных технологий, в различных сферах общественной жизни, усугубляется проблема борьбы с преступлениями, относящимися к компьютерной сфере. В зарубежных странах, с высоким уровнем компьютеризации, они уже давно являются одним из первичных направлений для криминологического исследования и разработки методик борьбы с ними и профилактики их предупреждения.

В России под компьютерной преступностью понимается совокупность компьютерных преступлений, где компьютерная информация является предметом преступных посягательств, а также преступлений, которые совершаются посредством общественно опасных деяний, предметом которых является компьютерная информация. Эти деяния посягают на безопасность сферы компьютерной информации, являются одним из наиболее опасных и вредоносных явлений современного мира[1].

С точки зрения уголовного законодательства Российской Федерации к компьютерным преступлениям относятся, во-первых, преступления в сфере компьютерной информации (ст. 272—274 УК РФ). Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, ст. 273 предусматривает ответственность и устанавливает наказание за создание, распространение и использование вредоносных программ для ЭВМ, ст. 274 устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Во-вторых, это все преступления, предусмотренные действующим УК РФ, совершающиеся в сфере компьютерной информации. Характерной особенностью многих компьютерных пре-

ступлений является то, что их предметом выступает компьютерная информация с целью приготовления к другим правонарушениям. В связи с этим недопустимо включать в компьютерные преступления только общественно опасные деяния, предметом которых является компьютерная информация.

Одной из основных проблем в расследовании преступлений в сфере компьютерной информации является трансграничность данной преступной деятельности. Если преступление совершается в пределах российской телекоммуникационной сети, то правоохранительные органы его, как правило, раскрывают. Если же преступник реализует свой замысел в различных сегментах сети Интернет, то расследование многократно затрудняется в связи с тем, что необходима помощь правоохранительных органов зарубежных стран.

Размытость определения компьютерной преступности является еще одной из проблем в борьбе с ней. Определение компьютерных преступлений как общественно опасных деяний, предметом либо орудием совершения которых являются средства вычислительной техники и компьютерная информация. Данная формулировка имеет слишком широкие и нечеткие границы в плане. Под нее подпадают многие преступления, в том числе и совершенно не имеющие отношения к преступлениям в сфере высоких технологий. Для примера: нанесение ноутбуком (переносным компьютером) тяжких телесных повреждений или умышленное уничтожение склада оргтехники. К компьютерным преступлениям, учитывая установленные в определении признаки, можно отнести клевету, распространенную через электронные средства информации, изготовление денежных знаков с помощью ксерокса и многое другое.

Совокупность преступлений в сфере компьютерной информации и опосредованных общественно опасных деяний образует другую часть компьютерной преступности. Симбиоз (сосуществование) этих общественно опасных деяний способен причинить значительный вред практически любым интересам личности, государства и общества. Данный симбиоз преступных деяний достаточно сложен для квалификации, и в большинстве случаев входящие в него противозаконные действия лиц, относящиеся к компьютерной сфере, остаются безнаказанными.

К другим проблемам борьбы с преступность в компьютерной сфере можно отнести:

— отсутствие отлаженной системы правового и организационно-технического обеспечения законных интересов граждан в области информационной безопасности (в нашей стране еще только проходят апробация и внедрение методов и средств по обеспечению интересов и прав граждан в области информационной безопасности, что является хорошей почвой для подготовки и совершения новых преступлений);

— недостаточное осознание органами государственной власти на федеральном и особенно региональном уровне возможных политических, экономических, моральных и юридических последствий компьютерных преступлений (из-за того, что во властных структурах всех уровней большинство составляют лица зрелого возраста от 50 лет, происходит двоякое отношение к компьютерной информации и последствиям ее неправомерного использования);

— слабость координации действий по борьбе с компьютерными преступлениями правоохранительных органов, суда и прокуратуры и неподготовленность их кадрового состава к эффективному предупреждению, выявлению и расследованию таких деяний (из-за упущения учебными заведениями компьютерной грамотности при подготовке сотрудников правоохранительных органов и судов мы получили ситуацию, когда без посторонней помощи следователи не могут квалифицировать и выстроить правильный план расследования деяний лиц из-за незнания понятийного и технического аппарата компьютерной сферы);

— серьезным отставанием отечественной индустрии средств и технологий информатизации и информационной безопасности от мирового уровня (ввиду малого финансирования данной сферы со стороны государства мы пришли к тому, что лица, совершающие противозаконные деяния в сфере компьютерных преступлений, превосходят технически органы, отвечающие за борьбу с ними).

Особое внимание должно быть уделено противодействию вовлечению молодежи в криминальную среду и разработке для нее эффективных методов воспитательной работы. В настоящее время происходит свободное распространение журналов и иных печатных изданий, в которых подробно описывается технология совершения компьютерных преступлений. Любой подросток, купив данное издание, может легко обучиться основным методам атак на информационные системы. В этой связи подрастающее поколение становится потенциальной угрозой для

безопасности компьютерных систем. В сети Интернет представлено более 2 740 000 сайтов, содержащих материал по методам совершения противозаконных деяний в сфере компьютерной информации, существуют форумы и виртуальные конференции с целью обмена опытом в совершении компьютерных преступлений. Таким образом, компьютерные преступники активно работают над улучшением своих навыков, вовлекают в участие в их среде подрастающее поколение, а также ведут активную деятельность по обучению и просвещению.

Нельзя не согласиться с мнением экспертов, которые считают, что следует совершить переход от иногда слабо связанных, противоречащих друг другу законов к целостному информационному кодексу. Таким образом, успешное осуществление этой работы будет способствовать повышению уровня правовой грамотности и правосознания пользователей инфотелекоммуникационными услугами, положительно повлияет на культурный уровень использования информационных технологий, позволит сократить риски массового использования телекоммуникационных сетей в противозаконных целях и будет способствовать достижению стабильности в инфотелекоммуникационной среде.

Успешное решение этих задач приведет к заметному увеличению раскрываемости преступлений, а также уменьшит количество преступлений, совершенных в сфере компьютерной информации.

Примечания

[1] Криминология : учебник для вузов / под общ. ред. д. ю. н., проф. А. И. Долговой. — 3-е изд., перераб. и доп. — М. : Норма, 2007. — С. 735.

СУХИХ И. И., аспирант ЧелГУ.

SUKHIKH I. I., Postgraduate Student of Chelyabinsk State University (ChelGU)

Центр по экспортному контролю ЮУрГУ

В соответствии с решением Комиссии по экспортному контролю Российской Федерации Южно-Уральский госуниверситет получил Свидетельство о специальном разрешении № 027 на осуществление деятельности по проведению независимой идентификационной экспертизы товаров и технологий в целях экспортного контроля.

В настоящее время ФГБОУ ВПО «Южно-Уральский государственный университет»(НИУ) располагает научно-педагогическим персоналом с высоким профессиональным и интеллектуальным уровнем, а также развитой лабораторной базой, это позволяет профессионально и качественно осуществлять деятельность по проведению независимой идентификационной экспертизы товаров и технологий, проводимой в целях экспортного контроля.

В соответствии с номенклатурой продукции, в отношении которой планируется осуществлять экспертизу, подобрано 107 экспертов, из них докторов наук 35, кандидатов наук 57 и 15 специалистов, не имеющих ученой степени. Все эксперты являются сотрудниками университета и способны квалифицированно и качественно провести экспертизу.

Если Вы являетесь поставщиками оборудования, машин, материалов, запасных частей и комплектующих для них, выпускаете сложную технику, научно-техническую продукцию и Вам приходится сталкиваться с терминами **«экспортный контроль»** и **«товары двойного назначения»,** то мы можем быть Вам полезны.

В соответствии с российским законодательством экспертизу товаров и технологий для целей экспортного контроля могут проводить только экспертные организации, получившие специальное разрешение Комиссии экспортного контроля Российской Федерации.

Центр по экспортному контролю ЮУрГУ осуществляет деятельность по проведению независимой идентификационной экспертизы товаров и технологий в целях экспортного контроля в отношении **продукции по всей номенклатуре действующих контрольных списков, утвержденных указами Президента Российской Федерации.**

Директор Центра:

Анатолий Григорьевич Мещеряков.

Тел.: (351) 267-95-49.

Заключения нашей экспертизы действуют на всей территории России и являются официальным документом, подтверждающим принадлежность или непринадлежность объекта экспертизы к продукции, включенной в списки контролируемых товаров и технологий.

Наши услуги:

1. Оформление заключений идентификационной экспертизы для целей **экспортного контроля** и таможенного оформления.
2. Консультация по **экспортному контролю** товаров (технологии).

Перечень документов, необходимых для проведения экспертизы:

1. Заявка.
2. Контракт (договор, соглашение).
3. Спецификация (перечень поставляемой продукции) и иные приложения.
4. Техническая документация (паспорта, сертификаты качества, руководства по эксплуатации, технические описания, этикетки и пр.).
5. Доверенность.

Наши координаты

Адрес: 454080, пр. им. В. И. Ленина, 85, корпус 3А, ауд. 502.
Телефон (351) 267-95-49
E-mail: exp-174@mail.ru
Транспорт (автобус, троллейбус, маршрутное такси):
остановка«ЮУрГУ»

ФИРМЕННЫЙ БЛАНК ОРГАНИЗАЦИИ

Исх. № _____
от «___» _____ 201__ г.

Директору Центра по экспортному
контролю ГОУ ВПО «ЮУрГУ»
А. Г. Мещерякову
454080, пр. им. В. И. Ленина, 85,
корпус 3А, ауд. 502

ЗАЯВКА
на проведение работ

Прошу Вас провести независимую идентификационную экспертизу товаров (технологий) в целях экспортного контроля и таможенного оформления.

Грузоотправитель: _____
_____
_____

Грузополучатель:_____
_____

Перечень поставляемой продукции:

№ п/п	**Наименование продукции**	**Единица измерения**	**Количество**	**Код ТН ВЭД**

Оплату работ по выставлению счета гарантирую.

Уполномоченный по техническим вопросам: _____
_____
_____

_____ _____ _____
(должность) (подпись) (Ф. И. О.)

Полезная информация

1. Экспертиза проводится в течение 3-х рабочих дней. По просьбе заказчика экспертиза может быть проведена в более короткие сроки.

2. Стоимость проведения экспертизы зависит от:

- ✓ объема рассматриваемого материала, продукции, информации, представленных согласно заявки;
- ✓ количества наименований товаров;
- ✓ количества кодов ТН ВЭД;
- ✓ сроков исполнения заявки;
- ✓ степени секретности материала, представленного на экспертизу.

3. Готовое заключение выдается на бумажном носителе (по просьбе заказчика — в электронном варианте).

4. Договор на оказание услуг заключается **каждый раз** в соответствии с заявкой.

Федеральные органы исполнительной власти

ФСТЭК России: http://www.fstec.ru/