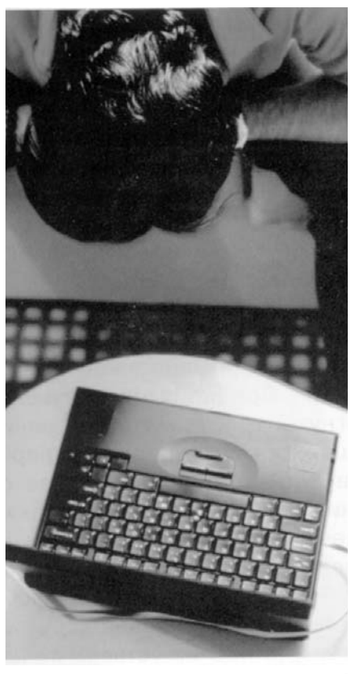


Информационная безопасность — вопрос выживания нации

Информация, как красивая женщина, — стоит дорого, принадлежит избранным и имеет право на свои секреты. А в современном обществе информация является еще и важным объектом правовых отношений. Технологическая революция в области информации, начавшаяся в последней трети XX века и продолжающаяся до сих пор, определила появление таких явлений, как «информационные войны» и «информационный терроризм».

Любой товар требует защиты

Война — дело государственное, в том числе и война информационная. Поэтому важное место в политике национальной безопасности в настоящее время занимает информационная безопасность. Вообще, технологическая революция в области информации связана прежде всего с развитием кибернетики, которое привело к созданию информационных систем управления. Вслед за этим повсеместно в массовом порядке стали внедряться персональные компьютеры, что в свою очередь повлекло за собой ускоренные темпы развития телекоммуникационных технологий. Затем персональные компьютеры стали объединять в компьютерные сети, вначале локальные, а затем и глобальные. Одновременно с колоссальным ростом популярности Интернета возникает беспрецедентная опасность разглашения персональных данных, критически важных корпоративных ресурсов. Кроме того, с каждым днем растет объем деловых операций, совершаемых через Интернет. Повышение информационной безопасности становится неотложной задачей, решения которой в равной мере требуют и конечные пользователи, и компании.

Новые виды вычислительной техники и связи создали уникальные возможности для включения информации в хозяйственный оборот и распространения на нее статуса товара. Информация превратилась в одно из важнейших средств воздействия на общественные отношения, стала одним из ценнейших товаров. Любой товар требует защиты, и особенной защиты требует такой «нематериальный» товар, как информация. Именно поэтому информационная безопасность в настоящее время является одной из самых развивающихся областей современной науки. Это в равной степени относится как к технической, так и к правовой стороне вопроса, касающегося информационной безопасности.

Практически каждый из нас в повседневной жизни сталкивается с результатами труда специалистов по информационной безопасности. Антивирусы, межсетевые экраны, авторизация и разграничение доступа, системы обнаружения и предотвращения атак, сканеры безопасности, системы контроля содержимого и антиспама — все это результаты развития технологий информационной безопасности.

Об актуальных проблемах обеспечения информационной безопасности России и путях их решения, а также о военно-техническом сотрудничестве нашей страны с иностранными государствами (ВТС России) рассказывает начальник департамента безопасности ФГУП «Рособоронэкспорт» Валерий ВАРЛАМОВ.

— Валерий Иванович, насколько актуальна сегодня проблема информационной безопасности государства?

— Актуальность этой проблемы подтверждается рядом факторов. Это все более активное воздействие на индивидуальное, групповое и общественное сознание через средства массовой информации; расширение информационного обеспечения органов государственного управления; создание инфраструктуры ситуационных и информационно-аналитических центров; необходимость обеспечения конфиденциальности информации; требования защиты информации и инфокоммуникационных систем; требования к достоверному, своевременному и эффективному прогнозированию, предупреждению и пресечению целенаправленного и опасного информационного воздействия на личность, общество и государство со стороны конкурентов, преступных или террористических группировок.

Для решения этих проблем недостаточно знаний в отдельной взятой информационной сфере. Необходимо четко представлять всю систему национальной безопасности, ее структуру, а также взаимосвязь и взаимовлияние угроз в различных сферах жизнедеятельности государства. Проблемы национальной безопасности не ограничиваются информационной сферой, а охватывают все сферы жизнедеятельности государства: политическую, экономическую, социальную, военную, культурную, духовную, демографическую, экологическую и другие.

НОВЫЕ УГРОЗЫ — НОВЫЕ ЗАДАЧИ

— Какие факторы обуславливают актуальность проблемы обеспечения информационной безопасности ВТС России?

— В настоящее время меры по обеспечению информационной безопасности ВТС России принимаются в соответствии с Концепцией национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 10.01.2000 г. № 24, и другими нормативными актами.

Актуальность обеспечения информационной безопасности ВТС России сегодня очевидна. Во-первых, значительно повысились требования к системному противодействию новым угрозам и к комплексному решению новых задач обеспечения информационной безопасности. Во-вторых, произошли серьезные изменения нормативной правовой базы в области информационной безопасности и ВТС: обострились угрозы утечки сведений, составляющих государственную, коммерческую и иную охраняемую законом тайну; и, наконец, сегодня стал жизненно необходим комплексный подход к построению и развитию системы обеспечения информационной безопасности ВТС России.

— Не могли бы вы сформулировать основную цель и основные задачи обеспечения информационной безопасности ВТС России?

— Еще в XVI веке государственный деятель и военачальник Оливер Кромвель точно отметил, что «дальше всех зайдет тот, кто не знает куда идти». Думаю, что знаменитый англичанин имел в виду следующее: чтобы определить направление пути, требуется обосновать не только основные цели и задачи, но и определить общую стратегию. Основной целью обеспечения информационной безопасности военно-технического сотрудничества является достижение экономической эффективности функционирования и устойчивости развития системы ВТС России при надлежащем соблюдении военно-политических интересов и выполнении международных обязательств Российской Федерации, а также повышение роли и места ВТС России в области внешнеторговой деятельности государства.

К основным задачам обеспечения безопасности ВТС России следует отнести:

1) развитие системы обеспечения безопасности ВТС России;

2) своевременное прогнозирование, выявление, предупреждение и пресечение внешних и внутренних угроз;

3) минимизация ущерба от непредотвращенных угроз, их локализация и нейтрализация;

4) организация и ведение научно-методической и информационно-аналитической деятельности в области обеспечения внутренней и внешней безопасности ВТС России, анализ деятельности конкурентов и проверка партнеров субъектов ВТС;

5) организация взаимодействия заинтересованных органов государственной власти, субъектов ВТС России по вопросам ИБ;

6) формирование сбалансированного законодательства в области ВТС, исключающего его неоднозначность, противоречивость и правовые пробелы;

7) развитие системы подготовки кадров по вопросам обеспечения информационной безопасности ВТС России, субъектов ВТС и других организаций;

8) сохранение высококвалифицированных кадров.

МЕТОДИКА «ДВОЙНЫХ СТАНДАРТОВ»

Уместно вспомнить, что существуют две группы объектов информационного воздействия: психологические и информационно-технические, которым соответствуют два вида информационной безопасности (ИБ).

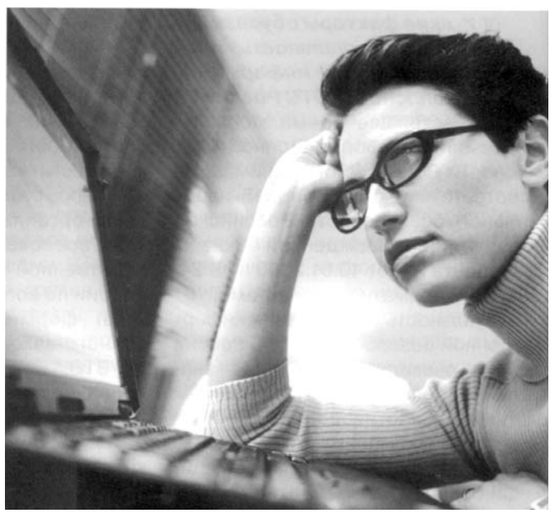
Информационно-психологическая безопасность — это вид ИБ, объектами защиты в которой являются психика (сознание, нервная система) отдельных людей, а также различные формы коллективного и общественного сознания (наука, духовная культура, мораль, идеология, религия, общественная психология и пр.).

Примеров деструктивного информационного воздействия можно привести множество. Вспомним, что первая попытка рассмотреть с научной точки зрения вопрос о действиях по разложению морального духа противника была предпринята в Китае около 500 лет до нашей эры в одном из древнейших трактатов по военному искусству. По мнению его автора Сунь Цзы, способы воздействия на моральные возможности противника сводятся прежде всего к деструктивному информационному воздействию.

ФЕДЕРАЛЬНЫЕ ЗАКОНЫ И КОНЦЕПЦИЯ ПРЕДПРИЯТИЯ

Информационно-техническая безопасность — это вид ИБ, объектами защиты в которой являются информационные и телекоммуникационные системы различного назначения. Информационные воздействия чреваты информационным ущербом не столько сами по себе, сколько тем, что запускают мощные вещественно-энергетические процессы и управляют ими.

В связи с этим ИБ следует рассматривать не только как самостоятельное явление,но и как аспект экономической, политической, научной, технологической, военной и других видов безопасности. Поэтому общей стратегией обеспечения ИБ ВТС России является достижение надежной и своевременной защиты интересов России от внешних и внутренних угроз, обеспечивающей реализацию государственной политики в области ВТС Российской Федерации с иностранными государствами.



«Среди пяти десятков угроз, которые реально осложняют военно-техническое сотрудничество России с иностранными государствами, около половины связаны с проблемой обеспечения информационной безопасности».

Научно-технический совет при ФГУП «Рособоронэкспорт».

— В решении каких задач по обеспечению информационной безопасности ВТС России удалось получить положительные результаты?

— Руководители и сотрудники заинтересованных органов государственной власти, субъектов ВТС и других организаций с гораздо большей ответственностью стали относиться к решению задач по обеспечению информационной безопасности на своих участках работы.

В последнее время удалось существенно продвинуться в решении ряда первоочередных практических задач:

1) по переходу от отдельных мероприятий к системе противодействия наиболее опасным угрозам, в том числе недобросовестной конкуренции;

2) по реализации положений Федерального закона «О коммерческой тайне»;

3) по внедрению новых технологий обеспечения информационной безопасности;

4) по организации научного подхода к обеспечению информационной безопасности ВТС России, субъектов ВТС и других организаций; а также в решении других актуальных задач.

— Каким направлениям деятельности по обеспечению информационной безопасности ФГУП «Рособоронэкспорт» вы уделяете особое внимание?

— В 2006 году изданы федеральные законы «Об информации, информационных технологиях и защите информации» (от 27.07.2006 г. №149-ФЗ) и «О персональных данных» (от 27.07.2006 г. №152-ФЗ). В соответствии с принятой законами терминологией обладателем информации, информационных ресурсов, формируемых на предприятии, является ФГУП «Рособоронэкспорт», и при осуществлении своих прав предприятие должно принимать меры по защите информации, а также ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

В рамках созданной на предприятии комплексной системы обеспечения безопасности информации особое место отводится следующим направлениям деятельности: безопасность документооборота, техническая защита информации, компьютерная безопасность, безопасность связи, а также информационно-аналитическая деятельность по указанным вопросам. В целом основные направления деятельности по обеспечению информационной безопасности предприятия отражены в концепции безопасности ФГУП «Рособоронэкспорт» и в программе ее реализации на период до 2009 года.

— Какие проблемы обеспечения информационной безопасности ФГУП «Рособоронэкспорт» являются в настоящее время наиболее актуальными?

— К основным следует отнести следующие проблемы. Во-первых, противодействие недобросовестной конкуренции со стороны зарубежных и российских субъектов ВТС и других организаций.

Типичным является пример двойных стандартов США. Вспомним о безосновательном протесте администрации США в связи с поставкой в Венесуэлу автоматов Калашникова. Вместе с тем США незаконно скупают калашниковых у третьих стран, в том числе в странах Европейского Союза. Одной из форм проявления недобросовестной конкуренции являются введенные экономические санкции США в отношении ФГУП «Рособоронэкспорт».

— Какие основные формы проявления недобросовестной конкуренции наиболее распространены?

— Форм недобросовестной конкуренции достаточно много. Среди основных можно назвать дискредитацию продукции военного назначения российского производства, субъектов ВТС, деятельности России в области ВТС; введение иностранных заказчиков в заблуждение относительно качества и тактико-технических характеристик ПВН; некорректное сравнение иностранным субъектом ВТС реализуемой ПВН с ПВН других субъектов ВТС; экспорт ПВН с незаконным использованием результатов интеллектуальной деятельности; незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную и иную охраняемую законом тайну.

— Какому направлению деятельности вы уделяете особое внимание в последнее время?

— Прежде всего мы уделяем внимание вопросам организации взаимодействия с органами государственной власти, субъектами ВТС, предприятиями и организациями оборонно-промышленного комплекса, структурными подразделениями предприятия, а также работе с кадрами. И не меньшее внимание мы уделяем проблеме формирования и развития системы научного подхода в обеспечении информационной безопасности. Без науки нельзя построить эффективную систему обеспечения информационной безопасности предприятия.

Мы исходим из того, что только единение теории и практики обеспечения информационной безопасности предприятия позволит достигнуть требуемого состояния защищенности интересов предприятия в информационной сфере от внешних и внутренних угроз, а также обеспечить стабильность функционирования и устойчивое развитие ФГУП «Рособоронэкспорт» и аффилированных с ним бизнес-структур в соответствии с их уставными целями и стратегией развития.

Федор НАДЫМОВ.

ОФИЦИАЛЬНО

Приложение к Указу губернатора Орловской области от 8 октября 2007 г. № 293

ПОЛОЖЕНИЕ
ОБ ОБЩЕСТВЕННЫХ ПРИЕМНЫХ ОРЛОВСКОЙ ОБЛАСТИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Общественные приемные — это внештатное объединение специалистов, представителей общественности, работающих на добровольной и безвозмездной основе по направлениям, соответствующим их профессиональным знаниям, образованию и опыту.

1.2. Общественные приемные в своей деятельности руководствуются Конституцией Российской Федерации, федеральными законами, правовыми актами Президента Российской Федерации и Правительства Российской Федерации, Уставом и законами Орловской области, правовыми актами губернатора и коллегии области и настоящим положением.

1.3. Методическое руководство общественными приемными осуществляется аппаратом губернатора и коллегии Орловской области.

1.4. Координация деятельности общественных приемных возложена на заместителя губернатора и председателя коллегии области — руководителя аппарата губернатора и коллегии области.

1.5. Общественная приемная и ее руководитель работают на общественных началах.

1.6. График работы общественных приемных вывешивается в местах их расположения, публикуется в средствах массовой информации.

2. СОСТАВ ОБЩЕСТВЕННЫХ ПРИЕМНЫХ

2.1. К работе в общественных приемных Орловской области могут привлекаться лица, обладающие специальными знаниями.

2.2. Экспертами в общественных приемных являются должностные лица органов государственной власти Орловской области, территориальных федеральных органов исполнительной государственной власти области, представители общественных институтов, периодически привлекаемые к работе в общественные приемные по мере необходимости, студенты.

2.3. Руководитель общественной приемной назначается указом губернатора области.

3. ОСНОВНЫЕ ЗАДАЧИ ОБЩЕСТВЕННЫХ ПРИЕМНЫХ

3.1. Создание единой системы распространения правовых знаний среди населения Орловской области.

3.2. Правовое просвещение населения области по вопросам прав и свобод человека, форм и методов их защиты и оказание помощи по правовым вопросам.

3.3. Обеспечение информационной открытости органов исполнительной власти Орловской области.

3.4. Разъяснение гражданам их прав и обязанностей.

3.5. Содействие эффективному взаимодействию населения, институтов гражданского общества, органов государственной власти области в решении вопросов обеспечения и защиты прав и свобод граждан.

3.6. Информирование населения области о политике, проводимой областной администрацией по вопросам социально-экономического развития.

3.7. Создание механизма участия граждан в совершенствовании деятельности государственных органов.

3.8. Общественные приемные области не представляют интересы граждан в судах и иных органах.

4. ОСНОВНЫЕ ФУНКЦИИ ОБЩЕСТВЕННЫХ ПРИЕМНЫХ

4.1. Организация правовой помощи населению и привлечение к работе в общественных приемных юристов и квалифицированных специалистов.

4.2. Информирование населения области об основных направлениях работы исполнительных органов государственной власти Орловской области.

4.3. Организация приема и консультирования населения по вопросам защиты прав и свобод человека и гражданина.

4.4. Анализ и обобщение обращений граждан, поступивших в общественные приемные, и регулярное информирование губернатора области о результатах деятельности общественных приемных.

4.5. Участие в подготовке проектов нормативных документов по вопросам защиты прав и свобод человека и гражданина.

4.6. Организация обучающих семинаров для населения по вопросам защиты прав и свобод человека и гражданина, разработка и распространение методических и консультационных материалов по вопросам защиты прав и свобод человека и гражданина.

4.7. Систематическое опубликование в средствах массовой информации материалов о работе общественных приемных.

5. ПОРЯДОК ПРЕКРАЩЕНИЯ ДЕЯТЕЛЬНОСТИ ОБЩЕСТВЕННЫХ ПРИЕМНЫХ ОРЛОВСКОЙ ОБЛАСТИ

Общественные приемные прекращают или приостанавливают свою деятельность на основании указа губернатора области.

КОЛЛЕГИЯ ОРЛОВСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

8 октября 2007 г. №230
г. Орел

О ПРОВЕДЕНИИ ОСЕННЕ-ЗИМНЕГО СЕЗОНА ОХОТЫ В 2007/2008 ГОДУ

Руководствуясь Федеральным законом от 24 апреля 1995 г. № 52-ФЗ «О животном мире», учитывая поступившие предложения охотопользователей, КОЛЛЕГИЯ ПОСТАНОВЛЯЕТ:

1. Разрешить проведение осенне-зимнего сезона охоты в 2007/2008 году: на лисицу красную — с 13.10.2007г. по 29.02.2008 г.; на куницу, хоря лесного (темного) и енотовидную собаку — с 1.11.2007 г. по 31.01.2008 г.; на зайца-русака — с 13.10.2007 г. по 30.12.2007 г. Дни охоты — четверг, пятница, суббота и воскресенье, а также другие дни недели, если они являются праздничными или объявлены выходными днями в установленном порядке.

2. Установить нормы добычи за день охоты: заяц-русак — 1 особь; лисица, куница, хорь и енотовидная собака — без ограничения норм добычи.

3. Запретить на территории области проведение охоты на барсука, норку, зайца-беляка, хоря степного (светлого), белку, ондатру.

4. Запретить охоту на все виды животных на территориях зелёных зон городов Орла и Болхова, охранных зон государственного мемориального природного музея-заповедника «Спасское-Лутовиново» Мценского района, государственного природного заповедника «Калужские засеки», государственных природных комплексных заказников «Кудияры» Залегощенского района и «Смирновский» Покровского района, природных парков Урицкого, Покровского и Свердловского районов, видовых государственных охотничьих заказников.

5. Опубликовать настоящее постановление в газете «Орловская правда».

6. Контроль за исполнением настоящего постановления возложить на первого заместителя губернатора и председателя коллегии Орловской области В.А. Кочуева.

Председатель коллегии Е.С. СТРОЕВ.