Л. А. Шивдяков (к. в. н.)
(ФСТЭК России, г. Хабаровск)

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЛЮЧЕВЫХ СИСТЕМАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КСИИ

В статье рассмотрены проблемы обеспечения информационной безопасности некоторых типовых объектов защиты Дальневосточного федерального округа, в составе которых функционируют информационно-телекоммуникационные системы, имеющие признаки ключевых (КСИИ). Проанализированы основные недостатки в организации мероприятий обеспечения безопасности информации (ОБИ) и технической защиты информации (ТЗИ) на объектах защиты, имеющих КСИИ, и сформулированы основные угрозы безопасности информации в КСИИ на основе современных методик и экспертных оценок инспекционных групп Управления ФСТЭК России по Дальневосточному федеральному округу.

1. Проблемы обеспечения информационной безопасности в ключевых системах информационной инфраструктуры (КСИИ) Дальневосточного федерального округа

Характерной особенностью функционирования органов государственного управления в настоящее время является внедрение в их деятельность новых информационных технологий, обеспечивающих получение и комплексный анализ значительных объемов объективной достоверной и своевременной информации, в том числе конфиденциальной информации и информации, составляющей государственную тайну, о реальном положении дел в различных отраслях и ведомствах, секторах экономики для поддержки управленческих решений. Комплексы и средства связи телекоммуникационной подсистемы различных уровней должны поддерживать реализацию современных информационных технологий электронного документооборота, организацию информационного обмена различными видами информации внутри каждого объекта системы, между отдельными объектами, информационными и ситуационными центрами органов государственной власти.

Естественно, что широкое внедрение в практику деятельности органов государственной власти, правоохранительных органов современных телекоммуникационных систем, в том числе с выходом в Интернет, средств электронно-вычислительной техники, специальных и других технических средств, как правило, иностранного производства, объективно ведет к увеличению вероятности утечки конфиденциальной информации.

Поэтому наметившееся интегрирование России в международные системы телекоммуникаций и информационного обмена невозможно без комплексного решения проблем информационной безопасности. Следует постоянно помнить о защите национальных и региональных информационных ресурсов и сохранении конфиденциальности информационного обмена по открытым сетям.

Следует учитывать, что управление оконечными коммутаторами существующих сетей передачи данных в России, и в ДФО в частности, производится с пунктов, расположенных в Москве. Хотя излишняя централизация информационного обмена перманентно создает более выгодные условия как для хищения закрытых сведений «в особо крупных размерах», так и для случайного или преднамеренного вывода всей информационной системы из строя. Разрушение годами накопленных данных или их модификация, приводящая к выдаче системой ложных сведений, может привести к исключительно большим экономическим и политическим потерям. Указанная ситуация возможна из-за отказов техники, а также в результате внедрения в систему так называемых программных закладок или компьютерных вирусов, других нежелательных воздействий. Поэтому одна из проблем в данной ситуации состоит в создании достаточно надежной защиты информационной системы от разрушения в случае воздействия на нее указанных факторов. Понятно, что, используя импортную аппаратную и программную базу, решить ее достаточно сложно.

Особенно благоприятная почва для распространения компьютерных вирусов, оказания иного нежелательного информационного воздействия появилась с созданием и непрерывным расширением сети Интернет и других открытых сетей подобного рода.

В ходе осуществления разрекламированной и весьма модной ныне «системной интеграции» фирмы, связанные, как правило, напрямую с крупными иностранными поставщиками оборудования и технологий, контролируемыми национальными спецслужбами, могут получить сопутствующую, в том числе и закрытую, информацию из банков данных государственных и других структур. Кроме того, «системный интегратор» зачастую является единственным, знающим все об информационно-коммуникационной системе, которую он создал, и он получает полный контроль над ней. При этом чаще всего потребителям предлагается интеграция их информационных ресурсов в Интернет или иные глобальные сети.

В связи с этим возрастает также возможность дистанционного конфигурирования программно-аппаратных средств информационно-коммуникационных сетей и управления ими по каналам связи. Поэтому довольно несложно организовать автоматизированный сбор необходимой информации, циркулирующей в российской системе, непосредственно из-за рубежа. Можно также создать условия, при которых информация будет передана адресату в искаженном виде, что, конечно, учитывая специфику сферы деятельности госструктур, повлияет на правильность принимаемых ими решений, особенно в критических ситуациях.

Естественный процесс информатизации органов власти и других государственных структур обусловил и появление новых видов угроз информационной безопасности, которые направлены, прежде всего, на системы управления и связи, системы жизнеобеспечения, ИТКС **критически важных объектов**, которые наиболее подвергнуты **деструктивным информационным воздействиям** — несанкционированным информационным воздействиям на информационную систему, приводящим к выводу системы из строя или к нарушению функционирования этой системы в результате разрушения (нарушения) ее информационно-технологической структуры.

В соответствии с разработанными признаками принадлежности объектов к критически важным и на основе анализа работы инспекционных групп управления, в общей структуре объектов Дальневосточного федерального округа нами выделено более 100 структур, в которых функционируют КСИИ. К основным из них относятся:

— ИТКС органов государственной власти и управления;

— ИТКС органов МВД и МЧС России;

— ИТКС таможенных органов, от работы которых зависит экономическая стабильность региона;

— ИТКС Дальневосточной железной дороги, а также Управления воздушным, морским и речным транспортом;

— ИТКС объектов энергетики, связи региона и других объектов.

Отсутствие должного внимания к обеспечению информационной безопасности этих систем может не только привести к потере государственного управления и огромному экономическому ущербу, но и оказать негативное воздействие на различные сферы деятельности общества и даже вызвать в ряде случаев катастрофические последствия.

Наиболее актуальными в настоящее время являются вопросы обеспечения безопасности информации в **ключевых системах информационной инфраструктуры**, расположенных в пределах федерального округа.

Определение: Основным признаком **ключевой системы информационной инфраструктуры (КСИИ) является ее** принадлежность к критически важному объекту, на котором имеется экологически опасное или социально значимое производство или технологический процесс, нарушение штатного режима которого приводит к чрезвычайной ситуации определенного уровня и масштаба, а также то, что если эта система (элементы системы) осуществляет функции управления чувствительными (важными) для Российской Федерации процессами, то нарушение ее функционирования приводит к значительным негативным для страны последствиям.

При этом не обязательно, чтобы в данных ИТКС обрабатывалась информация ограниченного доступа. В подобных системах может циркулировать **открытая информация**, например предназначенная для информирования граждан, или **технологическая информация**.

Соответствующими Указами Президента России (от 27 июля 2006 г. № 799 и от 30 ноября 2006 г. № 1321) на ФСТЭК России возложены дополнительные функции по реализации государственной политики в области обеспечения безопасности информации в КСИИ.

Изучая в течение довольно длительного времени состояние ОБИ и ТЗИ в ИТКС на объектах защиты федерального округа, сотрудники Управления ФСТЭК России по Дальневосточному федеральному округу пришли к выводу о том, что средства нападения злоумышленников на объекты информатизации (ОИ) и автоматизированные системы (АС) совершенствуются и выходят на более высокий качественный уровень значительно быстрее, чем развивается нормативная база и сами средства ТЗИ. В итоге процесс защиты информации приобретает пассивно-маловероятный характер, а выявление опасных каналов утечки информации и атакующей аппаратуры становится случайным успехом работников системы ТЗИ.

По результатам проведенных Управлением ФСТЭК России по ДФО за последнее время проверок состояния работ по обеспечению безопасности информации в КСИИ на объектах защиты федерального округа был выявлен ряд наиболее общих для всех проверенных структур недостатков:

· В большинстве ИТКС, имеющих в своем составе несколько подсистем различного уровня доступа, задачи комплексной защиты информации реализованы только в подсистемах верхнего уровня, обрабатывающих информацию ограниченного распространения либо управляющих технологическими процессами (АСУ-ТП). Это позволяет реализовать угрозу утечки охраняемых сведений путем программной логической обработки информации из открытых баз данных подсистем нижнего уровня. Такие данные, обобщенные и обработанные программно-аппаратными методами, формируют вполне определенную совокупность информации о всей ИТКС. Это может привести не только к потере сведений ограниченного распространения, но и к выявлению уязвимых звеньев системы для последующей разработки информационных атак на нее.

· В составе многоуровневых ИТКС в подсистемах верхнего уровня зачастую отсутствуют средства антивирусной защиты, а также средства контроля целостности системы, что мотивируется полной локальностью подсистемы и невозможностью удаленного доступа. При этом не учитывается так называемый человеческий фактор, возможность экстремистских и террористических проявлений. Имеется реальная вероятность несанкционированной установки вредоносных программ, способных воздействовать на основные программно-технические комплексы ИТКС, в том числе и автоматизированных систем управления технологическими процессами. Нарушение штатного функционирования таких систем способно привести к серьезным экологическим и социальным катастрофам.

· При проектировании и вводе в эксплуатацию ИТКС основные усилия многими организациями направляются на программно-техническое обеспечение, а вопросы обеспечения информационной безопасности остаются в стороне и не решаются в комплексе с вопросами информатизации.

Создаются высокотехнологичные, современные, но абсолютно незащищенные информационные системы, а после прилагаются огромные, «героические» усилия по их защите. И это притом, что способы реализации угроз информационной безопасности и формы их проявления постоянно совершенствуются, а система противодействия и так фактически только реагирует на возникающие угрозы и постфактум ищет способы их отражения.

Реалии сегодняшнего дня требуют создания «защищенных» ИТКС с интегрированной подсистемой безопасности информации, являющейся основой комплексной системы защиты и предполагающей использование разнородных средств и механизмов при построении целостной системы защиты. Эта система перекроет все существующие каналы угроз и обеспечит во всех компонентах ИТКС требуемый уровень безопасности информации, защиты от разрушающих воздействий, обеспечения живучести и устойчивости функционирования.

· Повсеместное использование в ИТКС иностранного оборудования и программного обеспечения, в первую очередь продукции компании «Майкрософт», и отказ от внедрения конкурентоспособных российских разработок на основе систем с открытым кодом представляют серьезную опасность обеспечению безопасности информации за счет возможного наличия в их составе программных и аппаратных закладок специального назначения и создания предпосылок не только к несанкционированному доступу к информации, но и к блокированию работы и выводу из строя оборудования ИТКС.

Вышеперечисленные недостатки стали следствием целого ряда проблем в развитии информационных технологий.

1. Одна из основных проблем вызвана высоким уровнем технологической зависимости в информационно-телекоммуникационной сфере. Это касается как технических средств, так и программного обеспечения, в первую очередь системного. Такая зависимость в некоторых секторах государственного управления может создать угрозу национальной безопасности.

Следует отметить, что индустрия информационной безопасности в большей степени, чем иные направления развития информационных технологий, сохранила высокий интеллектуальный потенциал и менее зависима от иностранного производителя. Российская отрасль информационной безопасности успешно решает новые задачи, возникающие в процессе развития информационного общества. Ряд организаций производит продукцию, способную конкурировать на мировом рынке.

2. Актуальной проблемой ОБИ в ИТКС на Дальнем Востоке России является усиление деятельности технических разведок по добыванию необходимой информации с использованием всего спектра возможностей, появляющихся в ходе экономического, технического и научного сотрудничества России с другими государствами, в том числе в ходе подготовки и проведения в 2012 г. в городе Владивостоке саммита АТЭС.

3. Еще одна проблема — это удовлетворение потребностей объектов защиты в высококвалифицированных специалистах в области ОБИ. Высокая технологичность современных угроз, применение для их нейтрализации современных средств защиты информации, постоянное развитие информационных технологий предъявляют достаточно высокие требования к квалификации специалистов по ОБИ. Недостаточная подготовка, незнание должностными лицами руководящих документов в области защиты информации и, как следствие, неправильное представление о принципах защиты и требованиях по созданию объектов информатизации способны подвергнуть риску нормальную работу предприятия и привести к необоснованным финансовым потерям.

4. Обеспечение безопасности ИТКС, находящихся на территории субъектов Федерации, осуществляющих межведомственное взаимодействие и обмен данными, управление предприятиями и организациями, в том числе теми, деятельность которых играет критически важную роль в поддержании нормальных условий жизни граждан, а также в обеспечении национальных интересов и безопасности в регионах, не может рассматриваться как проблема только тех организаций, которые занимаются их эксплуатацией и использованием. Это также и проблема региональной исполнительной власти.

5. Наметился целый ряд проблем, ставших актуальными в связи с использованием многими организациями сети Интернет в качестве телекоммуникационной составляющей создаваемых ИТКС. И хотя при этом требования Указа Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» в части подключения к сети Интернет информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, в которых циркулирует служебная информация ограниченного доступа, с использованием специально предназначенных для этого сертифицированных средств защиты информации в основном выполняются, при существующих и постоянно усложняющихся способах внешних воздействий на информационные системы игнорирование этих проблем недопустимо.

Наличие имеющихся проблем и указанных недостатков на объектах защиты свидетельствует о недостаточном внимании руководства организаций к вопросам обеспечения безопасности информации в ИТКС. Вследствие этого степень критичности КСИИ с учетом угроз безопасности информации не оценивается. Недостаточно уделяется внимания построению эффективной системы защиты информации в КСИИ[1].

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 1996 г. № 149-ФЗ. Ст. 3, 9, 16.
2. Федеральный закон «Об участии в международном информационном обмене» от 4 июля 1996 г. № 85-ФЗ. Ст. 9, 17.
3. Распоряжение Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации» от 9 сентября 2000 г. № р-1895.
4. Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 г. № 351.
5. Указ Президента Российской Федерации «Об утверждении Концепции национальной безопасности Российской Федерации» от 17 декабря 1997 г. № 1300. Разд. 2.
6. Постановление Совета Министров — Правительства Российской Федерации «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» от 15 сентября 1993 г. № 912-51. Разд. 1, ст. 9, 10; разд. 2, ст. 7; разд. 3, ст. 24, 25.
7. *Громыко И. А., Оспищев Е. Я., Кильмаев С. Ю.* Будущее за упреждающими системами защиты // Вопросы защиты информации. 2007. № 2. С. 11–14.

[1] Продолжение статьи в следующем номере.