Для увеличения $P_{НП}$ необходимо увеличивать среднее значение $M[t_{нп}]$ и уменьшать дисперсию $D[t_{нп}]$. Пути достижения этого достаточно подробно рассмотрены в [2] и заключаются, в основном, в усилении средств технической укрепленности. То есть в косвенном воздействии на преступника, вынуждающем его затратить больше времени на преодолении этих средств.

Использование нескольких рубежей охраны в каждой зоне позволяет существенно повысить вероятность обнаружения несанкционированных действий. Пусть P_1 , P_2 , P_3 – вероятности обнаружения проникновения ТС охраны соответственно для 1, 2 и 3 рубежей через интервал времени $T_{вi}$ после начала воздействия на контролируемый параметр i-го рубежа охраны. Вполне обоснованно можно предположить, что разные рубежи охраны используют извещатели с разным физическим принципом действия. Тогда можно считать, что события обнаружения проникновения извещателями каждого рубежа независимы и совместны. В этом случае вероятность обнаружения проникновения хотя бы одним рубежом системы сигнализации определяется известным выражением $P=P_1+P_2+P_3- P_1P_2- P_1P_3- P_2P_3+ P_1P_2P_3$. К примеру, при вероятности обнаружения каждым рубежом $P_i=0.8$, вероятность обнаружения системой сигнализации в целом составит 0,992. Однако, очевидно, что промежуток времени с момента начала воздействия на СТУ до обнаружения проникновения может заметно возрасти при пропуске нарушителя первым или первым и вторым рубежами. Это связано, во-первых, с более поздним воздействием на контролируемый параметр следующего рубежа и, во-вторых, с отличием во времени, необходимом для обнаружения проникновения извещателями с разным физическим принципом действия.

Таким образом наиболее эффективное решение задачи разработки системы защиты информации воз-можно лишь на основе интеграции объединенной системы обеспечения безопасности в целом, с использованием всех технических средств. Конкретные особенности, состав и условия функционирования ТСОБ будут зависеть от выявленных угроз. Целесообразно использование многозонной многорубежной охраны. Предложенный спо-соб позволяет получить оценку вероятности пресечения несанкционированных действий на охраняемом объекте.

Литература: 1. В.Волхонский, А.Засыпкин, В.Коротких. Структура технических средств обеспечения безопасности. БДИ //Безопасность, достоверность, информация. СПб., 1999, №3 ,С.18-20. 2. Н.В.Линев, А.А.Никитин, А.В.Климов. Раннее обнаружение несанкционированного проникновения //Системы безопасности, М., № 27, 1999, С.24 - 31. 3. В.В.Волхонский. Устройства охранной сигнализации. - СПб.: Экополис и культура, 1999. - 271 с.

УДК 659.2.002

КОНЦЕПЦИИ ЗАЩИТЫ ОТДЕЛЬНЫХ ОБЪЕКТОВ — НЕОБХОДИМАЯ СОСТАВНАЯ ЧАСТЬ НОРМАТИВНОЙ БАЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Виктор Маслак

Казенное предприятие "Харьковское конструкторское бюро по машиностроению имени А.А. Морозова"

Анотація: **В доповіді викладений один із шляхів удосконалення нормативної бази інформаційної безпеки держави. Обгрунтована необхідність розробки концепцій захисту окремих об′єктів, які є носіями таємної інформації.**

Summari: **The report expounds one of the possible ways of perfecting the normative base of informational security of the state, substantiates the necessity of development of conceptions of protection of separate objects which contain secret information.**

Ключевые слова: **концепция, информация, защита, объект.**

I Вступление

Со времени принятия Закона Украины "О государственной тайне" и создания Госкомсекретов Украины Указами Президента и постановлениями Кабинета Министров Украины утверждено и введено в действие много нормативно-правовых актов, которые сегодня составляют основу нормативной базы, обеспечивающей информационную безопасность государства. В то же время вряд ли кто возьмется определить исчерпывающий перечень нормативных документов, которые смогли бы в полной мере охватить все проблемы, связанные с охраной информации ограниченного доступа и прежде всего государственной тайны. Создание необходимой

нормативной базы является составной частью общегосударственного процесса построения системы защиты информации. Об этом говорит еще и тот факт, что, по данным зарубежных исследований, удельный вес нормативно-правовых, технических и организационных мер системы защиты информации соответственно составляет:

- нормативо-правовые — 60%;
- технические — 30%;
- организационные — 10%.

Из этого наглядно видно, что нормативно-правовые меры занимают лидирующее место по своей значимости и именно нормативно-правовое обеспечение должно рассматриваться как приоритетное направление в политике обеспечения информационной безопасности государства.

II Концепция защиты — путь совершенствования нормативной базы

Необходимость работы по совершенствованию уже имеющейся нормативной базы и разработке проектов новых нормативных документов вызвана постоянно происходящими изменениями в общественно-политических отношениях, развитием технических средств обработки и передачи информации, а в целом – ростом угроз для целостности информации.

Отрабатывая на местах вопросы практического обеспечения защиты информации с ограниченным доступом, особенно государственной тайны, наиболее полно ощущается нехватка того или иного инструмента для создания совершенного механизма защиты. Во многих случаях такой инструмент нужен не универсальный, а узконаправленный, специфический для того или иного объекта защиты. Рассматривая существующую сегодня нормативную базу по вопросам организации защиты информации с ограниченным доступом и в первую очередь носителей сведений, составляющих государственную тайну, ощущается нехватка документа, который бы определял стратегию, тактику и особенности защиты конкретного объекта защиты. Таким документом должна стать Концепция защиты конкретного объекта — носителя информации с ограниченным доступом.

Под объектом защиты будем подразумевать не абстрактное понятие, а комплекс физических, аппаратных и документальных средств, являющихся носителями информации ограниченного доступа, другими словами имеющими набор определенных сведений, подлежащих защите от несанкционированного доступа. Более конкретно это — система, образец, изделие, разработка военного или народно-хозяйственного, научного назначения, содержащие сведения, которые отнесены или могут быть отнесены в первую очередь к государственной тайне.

Что же такое Концепция защиты? Концепция защиты как система взглядов на цели, способы обеспечения безопасности информации и средства ее защиты должна в общем виде отвечать на три простых вопроса: что защищать; от чего защищать; как защищать?

Под вопросом "что защищать?" подразумевается в данном случае набор определенных сведений об объекте защиты и прежде чем ответить на него, необходимо четко разобраться, какие сведения подлежат защите.

Вопрос "от чего защищать?" связан с понятием "угроза". Угроза — потенциальная возможность неправомерного преднамеренного или случайного воздействия на объект защиты, приводящее к потере или разглашению секретной информации.

С вопросом "как защищать?" связано понятие "система защиты". Система защиты - это комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектов защиты.

Конкретизируя еще больше вышесказанное, необходимо сказать, что такие отдельные самостоятельные Концепции защиты должны быть разработаны для отдельных видов вооружения и военной техники (авиационные и ракетные комплексы, надводные корабли, танки, системы ПВО и т.д.), предприятий, деятельность которых связана с государственной тайной, систем связи и т.п.

III Необходимость разработки Концепции защиты отдельного объекта

На первый взгляд может показаться, что такой документ не нужен, так как существует достаточно нормативно-правовых документов, определяющих, что и как необходимо защищать. Это Закон Украины "О государственной тайне", "О защите информации в автоматизированных системах", Концепция национальной безопасности Украины, Концепция технической защиты информации, Свод сведений, составляющих государственную тайну Украины, Методические рекомендации госэкспертам по вопросам тайн по определению оснований отнесения сведений к государственной тайне и степени их секретности и т.д.

Однако, при более тщательном изучении опыта практического применения названных нормативных документов становится ясно, что это не так. Все они, вплоть до Свода сведений, составляющих гостайну, содержат общие формулировки с очень широкими границами применения того или иного положения.

У нас сегодня существуют к примеру документы, определяющие Концепцию защиты государства, это — "Концепция национальной безопасности" и "Оборонная доктрина", на основе которых строится вся система необходимых силовых структур, определяется необходимая численность, состав, оснащенность и Вооруженных Сил Украины, и СБУ и т.п. Однако, при этом у нас нет концепций защиты отдельных, наиболее важных и определяющих ячеек государства.

Если возвратиться немного назад, когда существовал Советский Союз, то многие, кто имел отношение к защите государственной тайны, вспомнят, что тогда существовали и использовались широко в практической работе разработанные Гостехкомиссией СССР Концепции противодействия иностранным техническим разведкам. Назову для примера несколько из них: особенности защиты военно-промышленных объектов, особенности защиты систем связи и АСУ, особенности защиты авиационных комплексов и т.д. Однако, ввиду тех глобальных преобразований, которые произошли и происходят в настоящее время, они уже не приемлемы к использованию в настоящее время. Но не воспользоваться опытом, наработанным в системе защиты государственной и военной тайны, которая существовала в стране до 1991 года и эффективности которой на Западе могли только позавидовать (об этом свидетельствуют многие мемуары наших "бывших" противников), было бы неразумно.

К слову, "Положение о Гостехкомиссии при Президенте Российской Федерации" от 19.02.99 г. определяет одной из функций Гостехкомиссии России разработку и утверждение концепций по технической защите информации.

Теперь попробую привести несколько практических примеров из опыта работы по защите информации, подчеркивающих необходимость разработки и утверждения таких Концепций.

Условиями предоставления разрешения (лицензии) на право осуществления деятельности, связанной с государственной тайной, предусмотрено определение категорий режима секретности предприятия, организации, деятельность которых связана с гостайной, а в самой форме лицензии необходимо указать эту категорию. О необходимости первоочередного нормативного решения этой проблемы (категорирования предприятий, организаций) говорилось и в докладах предыдущей подобной научно-технической конференции (доклад Ворожко В.П.). Кроме того, комиссии, проверяющие обеспечение защиты государственной тайны на предприятиях и в организациях, продолжают проверять и такое направление как "Защита предприятия как военно-промышленного объекта". С другой стороны отметим здесь еще тот факт, что предприятия ныне (разной формы собственности) ведут активную внешнеэкономическую деятельность и наряду с выполнением работ в интересах МО Украины ведут схожие работы и в интересах инозаказчика. Чем руководствоваться, определяя категорийность предприятия и что защищать на предприятиях, имеющих различную специфику? Ответить на эти и другие вопросы можно только при наличии тщательно отработанной Концепции защиты предприятий и организаций, деятельность которых связана с гостайной или может быть с ней связана (мобзадание на особый период).

Второй пример можно привести из практики работы Государственных экспертов по вопросам тайн, в части экспертизы и отнесения информации к государственной тайне. Неоднократно приходилось сталкиваться с ситуацией, когда несколько Госэкспертов, проводя независимо друг от друга экспертизу документов (материалов, подлежащих вывозу за рубеж, материалов заявок на изобретения, рассекречивание конструкторской документации) по военной технике по разному давали оценку степени секретности различным техническим характеристикам, решениям. Это значит, что ни "Свод сведений, составляющих гостайну", в существующем ныне виде, ни "Методические рекомендации Госэкспертам…" не позволяют однозначно определить «что защищать» по тому или иному изделию военной техники, НИР, ОКР. И в этом случае мы ощущаем нехватку именно Концепции защиты конкретного объекта.

Еще хуже обстоит дело с решением вопроса "от чего защищать?". Сегодня на предприятиях и в организациях, и то наверное далеко не на всех, имеется только "Модель ИТР-2000" ГТК СССР. Где-то, но не на предприятиях, как будто бы есть и "Модель ИТР-2010" украинского происхождения. Более рационально было бы перенести часть конкретной информации по возможностям ИТР из Модели в Концепцию, применительно к конкретному объекту защиты.

Такие Концепции должны быть разработаны применительно ко всему жизненному циклу объекта защиты и подвергаться корректировке в зависимости от общественно-политических, технических, экономических и других факторов, влияющих на информационную безопасность государства. Кроме того, они не должны сводиться только к технической защите и только для защиты от технических средств, а рассматривать понятие защиты в более широком смысле этого слова.

IV Выводы

1 Для правильного подхода к защите информации ограниченного доступа, в особенности государственной тайны, необходима разработка и утверждение Концепций защиты конкретных объектов, являющихся носителями такой информации.

2 Соответствующим подразделениям СБУ, совместно с министерствами, ведомствами, ведущими предприятиями, организациями, НИИ, КБ Украины необходимо провести работу по разработке Концепций защиты наиболее важных объектов.

Литература: *1. Закон Украины "О государственной тайне". 2. Свод сведений, составляющих государственную тайну Украины. 3. Правове, нормативне, та метрологічне забезпечення систем захисту інформації в Україні// Матеріали ювілейної науково-технічної конференції. - Київ, 1998. 4. Указ Президента РФ № 212 от 19.02.99г. "Положение о Государственной технической комиссии при Президенте Российской Федерации". 5. Каторгин Ю.Ф. и др. Энциклопедия промышленного шпионажа. - С.-Петербург: Полигон, 1999. 6. Концепция технической защиты информации в Украине. 7. Методические рекомендации государственным экспертам по вопросам тайн по определению оснований для отнесения сведений к государственной тайне и степени их секретности.*

УДК 621.96

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЕОМ ДЛЯ ОБРОБКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В СУЧАСНИХ УМОВАХ

Георгій Левченко, Михайло Ільченко, Володимир Хорошко, Валерій Буркацький, Костянтин Золотухін, Володимир Грошев

Науково-виробниче підприємство "Плазмотехніка", Національний технічний університет України "КПІ", Київський міжнародний університет цивільної авіації, Генеральний штаб Збройних Сил України, Державний упроваджувальний центр "Спецтехніка" МВС України

Анотація. **Розглянуто проблеми захисту інформації від витоку по ПЕМВН та електромагнітного тероризму. Проаналізовані особливості застосування екранованих приміщень та генераторів шуму. Запропоновані організаційні заходи щодо підвищення рівня інформаційної безпеки державних органів та критичних інфраструктур з використанням ЕОМ в захищеному виконанні за ГОСТ29339. Сформульовані пропозиції можуть бути використані банками та іншими небайдужими до захисту інформації організаціями.**

Summary. **Problems of protection of information from leakage by electromagnetic emanation and from electromagnetic terrorism are considered. Features of application of shielded premises and generators of a noise are analyzed. Organizational measures on rise of a level of information safety of state bodies and critical infrastructures with use of computers in protected fulfillment by GOST29339 are offered. Use of suggestions by banks and other not indifferent to protection of the information organizations is possible.**

Ключові слова: **захист, інформація, екранування, випромінювання, норми.**

Впровадження в усі сфери життєдіяльності держави інформаційних технологій зумовило розширення сфери застосування ЕОМ для обробки інформації з обмеженим доступом (ІзОД). Така інформація в наш час потребує додаткового підвищення ступеня захищеності як від перехоплення її по побічних електромагнітних випромінюваннях та наводах (ПЕМВН), так і від навмисного силового електромагнітного впливу, який може спотворити її або зовсім знищити.

Завдяки науково-технічному прогресу сучасні засоби перехоплення інформації якісно відрізняються від тих, на які орієнтована чинна нормативна база в галузі технічного захисту інформації. Так, сучасна портативна апаратура перехоплення своїми можливостями відповідає стаціонарній 70-х років, а за деякими характеристиками перевищує останню.

Цифрова обчислювальна техніка дозволяє реалізувати оптимальний прийом та забезпечити накопичення будь-якої достатньої кількості повторів для відновлення перехопленої інформації не апаратними засобами, як раніше у стаціонарних комплексах радіо- та радіотехнічної розвідки, а на рівні програмного забезпечення.

Значне покращення характеристик радіоприймальних пристроїв (зокрема, зниження рівня власних шумів, підвищення чутливості, різке зменшення габаритів і маси) і використання малогабаритних ЕОМ з відповідним програмним забезпеченням дозволяють створити портативні системи з реалізацією на одній і тій самій апаратній