УДК 004.322

Г.Н. Розоринов

ТЕКУЩЕЕ СОСТОЯНИЕ РАЗВИТИЯ СОВРЕМЕННЫХ СИСТЕМ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ ВЛИЯНИЕ НА ЭКОНОМИКУ ГОСУДАРСТВА

Показано, что защиту информации следует рассматривать с привязкой не к субъектам, а к сферам деятельности, независимо от того, ко всем или к одному субъекту относятся эти сферы деятельности. При этом значение защиты информации определяется через те последствия, которые наступают в результате защиты или при ее отсутствии. Анализируется система подготовки, переподготовки и повышения квалификации специалистов по защите информации.Утверждается, что повышение безопасности информационных систем приводит к увеличению роста ВВП, международной торговли страны, экспорта, производительности труда граждан, числа рабочих мест, а также добавленной стоимости в год.

Ключевые слова: защита информации, принципы организации, нормативно-правовая база.

Введение

Информация приобрела статус стратегического национального ресурса, являющегося одним из основных богатств государства, претендующего на достойное место в международном сообществе [1,2]. Активное внедрение информационных технологий в самых разных областях жизнедеятельности Украины наряду с несомненно положительными тенденциями несет в себе определенные проблемы, одной из которых является обеспечение режима безопасности в информационно-коммуникационных системах (ИКС). К одной из проблем относится рост трафика.

На сегодняшний день средняя скорость домашнего подключения в США составляет 25 Мбит/с, и 20% всех американских домохозяйств с широкополосным интернетом имеют скорость подключения уровня Т3 и выше, причем канал предоставляется только лишь обитателям данного жилища. Можно сравнить эти цифры с показателями двадцатилетней давности, тогда весь глобальный интернет-трафик составлял 15 ГБайт в месяц. В 2014 г. интернет-трафик вырос, по сравнению с 1984 г. в 2,7 миллиарда раз.

Однако, при анализе роста интернет-трафика брать за точку отсчета 1984 г. не совсем справедливо: природа коэффициентов роста такова, что в первые несколько лет они будут гигантскими для любого, даже не самого успешного продукта или отрасли, ибо рост начинается с нуля. Поэтому рационально взять в качестве отправной точки не 1984-й, а 2000-й г. Но и он, с точки зрения интернет-трафика, кажется далеким прошлым: в 2014 г. интернет-трафик был в 564 раза больше трафика 2000 г (табл. 1).

Таблица 1

Рост некоторых мировых показателей

Показатели	2000	2014	Рост, %
Средняя стоимость авиабилета на внутренние рейсы (долл. США)	339	392	16
Население нашей планеты, млрд.	6,1	7,2	18
Сумма кассовых сборов в кинотеатрах США (млн. долл.)	7 661	10 361	35
Галлон молока (США), долл.	2,79	3,82	37
Реальная стоимость доллара (США)	1	1,37	37
Стоимость билетов в кино (США), долл.	5,39	8,17	52

Потребление электричества (во всем мире), млрд. кВт	13 246	20 450	54
Мировой ВВП (млрд. долл.)	33 181,87	77 301,96	133
Средняя рабочая частота процессора (США), МГц	450	2 400	433
Пользователи сотовой связи (во всем мире, включая голосовые звонки), млрд.	0,738	4,3	477
Пользователей Интернета (во всем мире), млрд.	0,304	2,8	826
Средний размер жесткого диска на ПК (США), ГБ	10	250	2400
Объем интернет-трафика на одного пользователя (во всем мире), ГБ/мес	0,247	15,1	5990
Глобальный объем интернет-трафика (во всем мире), ГБ/мес	75 250 000	42 423 431 275	5627

В таблице безоговорочно лидирует интернет-трафик. Интернет-трафик показывает не только максимальный рост числа пользователей и устройств, но и рост частоты использования, тенденций применения и повышение пропускной способности каналов.

Важно отметить, что самый загружающий процесс для канала — это перемещение файлов: мгновенное перемещение файлов требует высокой пропускной способности. Чтобы переместить файл объемом 10 ГБайт за несколько минут, требуется 300 Мбит/С, а чтобы передать файл в 1 ГБайт за 4 С, требуется скорость в 2 Гбит/С. Мгновенное перемещение файлов необходимо для корректной работы облачных приложений, резервного копирования в режиме реального времени и облачного хранилища, а также определенных типов удаленной работы, требующей обработки большого количества данных.

Основная часть

Основными свойствами информации и систем ее обработки, которые должны поддерживаться в ИКС, являются доступность, целостность и конфиденциальность(рис. 1).

Рис. 1. Свойства информации

Как конкретно должна быть организована защита ИКС, единого мнения до сих пор несуществует[3 -5]. Это обстоятельство объясняется тем, что наука о защите информации в ИКС сравнительно молода, и необходимая теоретическая база просто не успела сформироваться.

Тем не менее, сложились основные понятия, используемые в сфере обеспечения информационной безопасности: политика безопасности, подотчетность и гарантии.

Главная цель создания системы защиты информации (СЗИ) - достижение максимальной эффективности защиты за счет одновременного использования всех

необходимых ресурсов, методов и средств, исключающих несанкционированный доступ к защищаемой информации и обеспечивающих физическую сохранность ее носителей.

Осуществление мероприятий по защите информации носит массовый характер, занимается этой проблемой большое количество специалистов различного профиля. Но успешное осуществление указанных мероприятий при такой их масштабности возможно только при наличии хорошего инструментария в виде методов и средств решения соответствующих задач[6]. Разработка такого инструментария требует наличия развитых научно-методологических основ защиты информации (рис. 2).

Рис. 2.Научно-методологические основы защиты информации

СЗИ относится к системам организационно-технологического (социотехнического) типа, так как общую организацию защиты и решение значительной части задач осуществляют люди (организационная составляющая), а защита информации осуществляется параллельно с технологическим процессом ее обработки (технологическая составляющая). Она характеризуется рядом признаков (рис. 3):

Рис. 3. Признакисистемы защиты информации

СЗИ - сложная система, функционирующая, как правило, в условиях неопределенности, требующая значительных материальных затрат. Поэтому определение основных принципов СЗИ обусловливает основные подходы к ее построению (рис. 4).

Поскольку СЗИ предназначена обеспечивать безопасность всей защищаемой информации, к ней должны предъявляться требования, показанные на рис. 5.

На всем протяжении существования компьютерных технологий идет непрерывное изменение взглядов на вопрос обеспечения безопасности в ИКС[2-5]. Первые попытки создания режима информационной безопасности в ИКС были предприняты еще в 60-е годы. Основной идеей этого этапа было создание средств, позволяющих обеспечивать надежную защиту информации механизмами, содержащими в основном технические и программные средства. При этом господствовало мнение, что основными средствами защиты информации являются программные, причем считалось, что такие средства будут работать эффективнее, если будут включены в состав операционной системы (ОС).

В Украине, также как и в других государствах, привычным для потребителей стало вместе с приобретением ОС получать готовую возможность обеспечить безопасность собственных информационных ресурсов. Считалось, что этого достаточно.

Рис. 4. Основные подходы к построению СЗИ

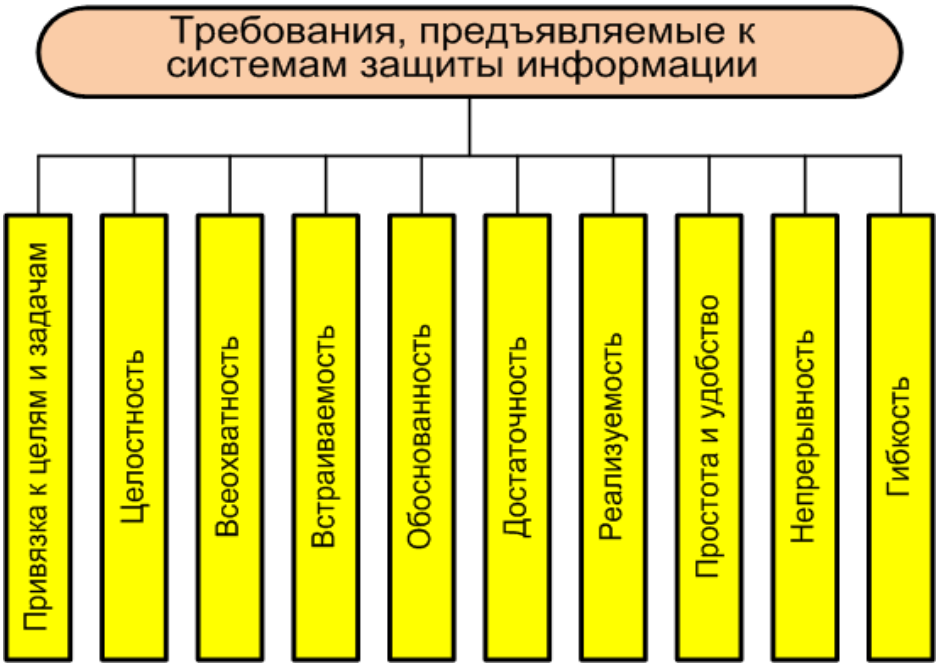

Рис. 5. Требования, предъявляемые к системам защиты информации

Под безопасностью ОС принято понимать такое ее состояние, при котором невозможно случайное или преднамеренное нарушение функционирования ОС, а также нарушение безопасности находящихся под управлением ОС ресурсов системы.

Можно выделить функциональные дефекты ОС различных типов, которые могут привести к созданию каналов утечки данных(рис. 6):

Рис. 6. Функциональные дефекты ОС различных типов

Идентификация. Каждому ресурсу в системе должно быть присвоено уникальное имя - идентификатор. Во многих системах пользователи не имеют возможности удостовериться в том, что используемые ими ресурсы действительно принадлежат системе.

Пароли. Большинство пользователей выбирают простейшие пароли, которые легко подобрать или угадать. Согласно опросу, проведенному компанией LaunchKey, занимающейся мобильной аутентификацией, 84% пользователей хотели бы заменить пароли на другие способы авторизации. В качестве таких примерно три четверти опрошенных назвали сканирование лица, сетчатки глаза, или отпечатков пальцев.

Как показали результаты опроса, большинству пользователей не нравится требование большинства систем авторизации использовать пароли определенной сложности, а также необходимость периодически их менять.52% респондентов ответили, что они используют менее 10 паролей, и постоянно чередуют их на различных сайтах, приложениях и ОС.

Лишь 22% пользователей утверждает, что всегда могут вспомнить свои пароли. Те, кто не могут этого сделать, пользуются сбросом пароля по ссылкам на сайтах (31%), либо прибегают к спасательной бумажке, на которой пароль был заранее записан.

Что касается двухфакторной аутентификации, то 53% не знает что это такое, 20% никогда не использовали этот тип защиты, 16% применяет лишь на некоторых сайтах, и только 9% активирует 2FA везде, где есть такая возможность.

Список паролей. При хранении списка паролей в незашифрованном виде возникает возможность его компрометации с последующими попытками несанкционированного доступа к данным.

Пороговые значения. Для предотвращения попыток несанкционированного входа в систему с помощью подбора пароля необходимо ограничить число таких попыток, что в большинстве ОС не предусмотрено.

Подразумеваемое доверие. Во многих случаях программы ОС выполняются из расчета, что другие программы работают правильно.

Общая память. При использовании общей памяти не всегда после выполнения программ очищаются участки оперативной памяти (ОП).

Разрыв связи. В случае разрыва связи ОС должна немедленно закончить сеанс работы с пользователем или повторно установить подлинность субъекта.

Передача параметров по ссылке, а не по значению. В связи с тем, что при передаче параметров по ссылке параметры могут быть оставлены в ОП после проверки их корректности, нарушитель может изменить эти параметры до начала их использования системой.

Практика использования современных ОС показала, что надежность механизмов защиты, реализованных в них, явно недостаточна. Уж если основатель и главный разработчик корпорации Microsoft Билл Гейтс публично признал, что многие продукты своей компании, возможно, придется полностью переделать, то не приходится сомневаться в необходимости использования специализированных средств защиты информации. По мнению Гейтса, теперь компьютеры должны быть не просто безопасными, они должны быть такими, чтобы им можно было всецело доверять.

А пока, как показывает опыт отечественных разработок средств защиты информации, оптимальным и достаточно надежным способом обеспечения безопасности информации является использование специальных недорогих плат, устанавливаемых в один из слотов системной платы. Обычно, имеющийся на плате чип содержит дополнительный блок BIOS, который вступает в действие после окончания работы основного и разрешает загрузку компьютера только с жесткого диска.

Таким образом, сегодня "основной вопрос" информационной безопасности - что первично "hard" или "soft"успешно решается на основе применения специализированных средств защиты информации, целостность которых обеспечивается технологией производства и периодическими проверками.

Полезно обратиться к мировому опыту. Так, например, Эстония — страна, хорошо известная специалистам-технологам, заслужила репутацию высокоразвитой державы. Во многом благодаря выходцам из Эстонии мир увидел незаменимые нынче технологии, такие как Skype, Nokia, Ericsson, Kazaa, MySQL и многие другие.

Даже хэш-тег #Estonianmafia был придуман Дэйвом МакКлюром, основателем более пятисот стартапов и суперинвестором, в 2011 году во время проведения британским акселератором Seedcamp финала конкурса стартапов в Лондоне, когда он заметил, что четыре из 20 команд-участниц были из Эстонии.

Эстония – одна из первых стран, в которой стали применяться электронные удостоверения личности (ID-карты). Карта является действительной в пределах государства, а также во всех странах Евросоюза. Эстонская ID-карта удостоверяет личность владельца в реальном и цифровом пространстве.Во встроенном чипе находится информация о личности и электронная подпись. Помимо этого карта может хранить в себе криптографические ключи и различные сертификаты и документы. Владелец может предъявить эту карту в аптеке, чтобы получить прописанные лекарства или использовать в общественном транспорте для оплаты проезда. Сейчас ID-карты используют 90% населения, то есть она не является обязательной для жителей страны. Именно эстонскую систему электронных паспортов считают образцовой.

Однако, несмотря на практичность таких паспортов, у них есть один серьезный недостаток, а именно защита. В 2012 году одну из карт удалось взломать всего за 13 минут, что заставило разработчиков серьезно задуматься о повышении безопасности.

Эстония ушла далеко вперед в плане внедрения информационных технологий и интернета в жизнь. У этой небольшой страны, в которой проживают по данным на 2012 год - 1,339 миллионов человек, можно многому поучиться в плане развития и внедрения технологий. При этом, приоритетным направлением стала задача эффективного государственного управления и инструментом его достижения стал проект государственного масштаба "Электронная Эстония" (рис. 7).

В итоге государственные органы получили электронный инструмент обслуживания населения и скорость обслуживания населения выросла в несколько раз.

Эстонцы отметили следующие эффекты интернетизации:

- увеличение на 10% подключений граждан к скоростным интернет-магистралям в обществе увеличивает рост ВВП на 1,4%, в Евросоюзе 3,4% роста ВВП относят к непрерывной интернетизации;
- с интернетизацией в 10% международная торговля страны растёт в 1,9 раза, экспорт увеличивается в 2,1 раза, производительность труда граждан растёт на 15%;
- интернетизация даёт прирост на 2,6 рабочих места на одно потерянное рабочее место, в связи с автоматизацией и сокращением штатов в государственном аппарате, и один компьютеризированный и подключённый к сети работник производит на 500$ больше добавленной стоимости в год.

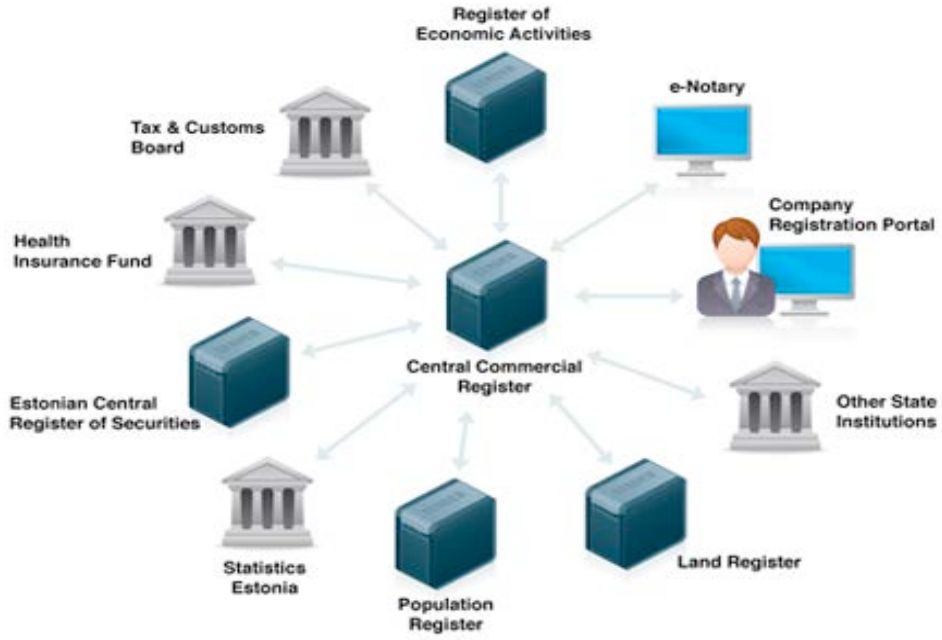

Рис. 7. Проект государственного масштаба "Электронная Эстония"

Но чтобы развить возможность оплаты государственных услуг через Интернет, платить налоги и иные платежи, была введена банковская электронная авторизация. Сейчас 75% госуслуг признают банковскую интернет-транзакцию. Каждому банку и каждому гражданину были выданы персональные карточки, которые были привязаны к единому идентификационному номеру гражданина (рис. 8)

. Рис. 8. Персональная карточка и паспорт гражданина Эстонии

Появилась реальная возможность для практического использования электронно-цифровой подписи. 10 октября 2011 года было поставлено 64 млн. цифровых подписей, которая стоит порядка 25 евро.

Сердцевиной "Электронного государства" Эстонии является X-tee/X-Road. Это электронная среда обмена данными между различными информационными системами.

В Эстонии действует и электронная полиция. Все камеры видеонаблюдения, базы данных по книге учёта преступлений, база данных преступников, жертв преступлений хранится в этом портале. Её работа привела к снижению статистики ежегодных убийств до нуля к 2010-му году. Теперь полиция работает на упреждение и профилактику преступности.

Начиная с 1995 года Интернет банки Эстонии 99% всех банковских операций проводят через интернет, тогда как в Евросоюзе всего 44%, а в США – 38%. Скандинавские центры э-банкинга расположены в Эстонии. Все банки в Эстонии имеют централизованную интернет-среду, а также и среду в мобильном интернете. Мобильный телефон у эстонцев – это и паспорт, и кошелёк, и офис, и полиция.

В учебных программах ведущих университетов Эстонии также подчеркнута ценность инноваций.

С 1 января 2016 года в Украине также можно будет заменить внутренний паспорт ID-картой. Для этого создается национальная система идентификации. Цель – это построение новой системы идентификации, обеспечения национальной безопасности. Карты будут выдавать с 14 лет. Внутренние паспорта-карточки будут оформляться по тому же принципу, что и заграничные биометрические паспорта (рис. 9).

Рис. 9. Внутренний паспорт-карточка гражданина Украины

Новая система идентификации будет опознавать личность с персональными данными, фото, биометрическими данными, а граждане получат современные защищенные документы. Их в свою очередь можно будет оформить через портал Государственной миграционной службы и единый государственный портал административных услуг.

Оформление ID-карты будет проводиться по желанию, и не является обязанностью.

Значение защиты информации определяется не только в системе информационной безопасности, но и в системе национальной безопасности.

Цели защиты информации для государства, общества и отдельных личностей различны. Они в конечном итоге дополняют друг друга и каждый из субъектов объективно заинтересован в защите информации других субъектов. В различных сферах деятельности интересы всех субъектов должны или совпадать или дополнять друг друга. С учетом этого защиту информации следует рассматривать с привязкой не к субъектам, а к сферам деятельности независимо от того ко всем или одному субъекту относится эти сферы деятельности. При этом значение защиты информации целесообразно определить через те последствия (положительные или отрицательные), которые наступают в результате защиты или при ее отсутствии:

1. В области внешней политикизащита информации обеспечивает свои внешне - политические интересы, т. е. иметь преимущества над другими государствами. Достигаются с помощью секретно-сепаратных договоров о военно-политическом сотрудничестве. Защита информации повышает политический уровень такого государства и его международный авторитет. Защита информации может давать и отрицательный результат : если предоставить очень большой объем закрытой информации, во внешней политике это может привести к осложнению в области международной политики.

2. В военной области защита информации позволяет сохранить в тайне от потенциального противника сведения о составе военной техники, ее количестве, тактики, технических данных о разработке новых систем оружия и военной технике, об организации обороны подготовке на случай войны. С другой стороны чрезмерная закрытость информации о вооружении вызывает сомнения других государств, приводит к гонке вооружений. Неоправданный объем защищенной информации в этой области сокращает возможность использования научно-технических достижений в гражданских областях экономики.

3. В экономической сфере деятельности защита информации дает возможность иметь высокие доходы, сохранять приоритет, заключать выгодные контракты, добиваться преимущества над конкурентами, избегать экономического ущерба. Излишняя засекреченность в экономике снижает доверие к ее отраслям или предприятиям со стороны потенциальных партнеров и потребителей продукции, тормозит инвестиции и подрывает престиж предприятия.

4. В социальной сфере - в политических, экономических, правовых и других областях, определяющих общественную и частную жизнь человека защита информации направлена на улучшения морального и материального благосостояния человека.

Меры обеспечения сохранности и защиты информации в государственной организации, на предприятии или фирме различаются по своим масштабам и формам. Они зависят от производственных, финансовых и других возможностей, от количества охраняемых секретов и их значимости. При этом выбор таких мер необходимо осуществлять по принципу экономической целесообразности, придерживаясь в финансовых расчетах "золотой середины", поскольку чрезмерное закрытие информации, так же как и халатное отношение к ее сохранению, могут вызвать потерю определенной доли прибыли или привести к непоправимым убыткам. Отсутствие у руководителей предприятий четкого представления об условиях, способствующих утечке конфиденциальной информации, приводят к ее несанкционированному распространению.

Наличие большого количества уязвимых мест на любом современном предприятии или фирме, широкий спектр угроз и довольно высокая техническая оснащенность злоумышленников требует обоснованного выбора специальных решений по защите информации. Основой таких решений можно считать:

• Применение научных принципов в обеспечении информационной безопасности, включающих в себя: законность, экономическую целесообразность и прибыльность, самостоятельность и ответственность, научную организацию труда, тесную связь теории с практикой, специализацию и профессионализм, программно-целевое планирование, взаимодействие и координацию, доступность в сочетании с необходимой конфиденциальностью;

• Принятие правовых обязательств со стороны сотрудников предприятия в отношении сохранности доверенных им сведений;

• Создание таких административных условий, при которых исключается возможность кражи, хищения или искажения информации;

• Правомерное привлечение к уголовной, административной и другим видам ответственности, которые гарантируют полное возмещение ущерба от потери информации;

• Проведение действенного контроля и проверки эффективности планирования и реализации правовых форм, методов защиты информации в соответствии с выбранной концепцией безопасности;

• Организация договорных связей с государственными органами регулирования в области защиты информации.

Вопрос обеспечения информационной безопасности сегодня для Украины стоит на одном уровне с защитой суверенитета и территориальной целостности, обеспечением ее экономической безопасности. Уровень информационной безопасности активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности Украины, потому что чаще всего реализация информационных угроз - это нанесение вреда в политической, военной, экономической, социальной, экологической сферах.

Среди угроз национальной безопасности Украины в информационной сфере определены угрозы, связанные с разглашением информации, которая составляет государственную и другую, предусмотренную законом, тайну, а также служебной (конфиденциальной) информации, которая направлена на обеспечение потребностей и национальных интересов общества и государства, а также угрозы, связанные с компьютерной преступностью и компьютерным терроризмом.

Именно с целью противодействия отмеченным угрозам и необходимостью снижения уровня вероятности их реализации и нежелательных последствий, в Украине создана и функционирует система технической защиты информации [7] (рис. 10).

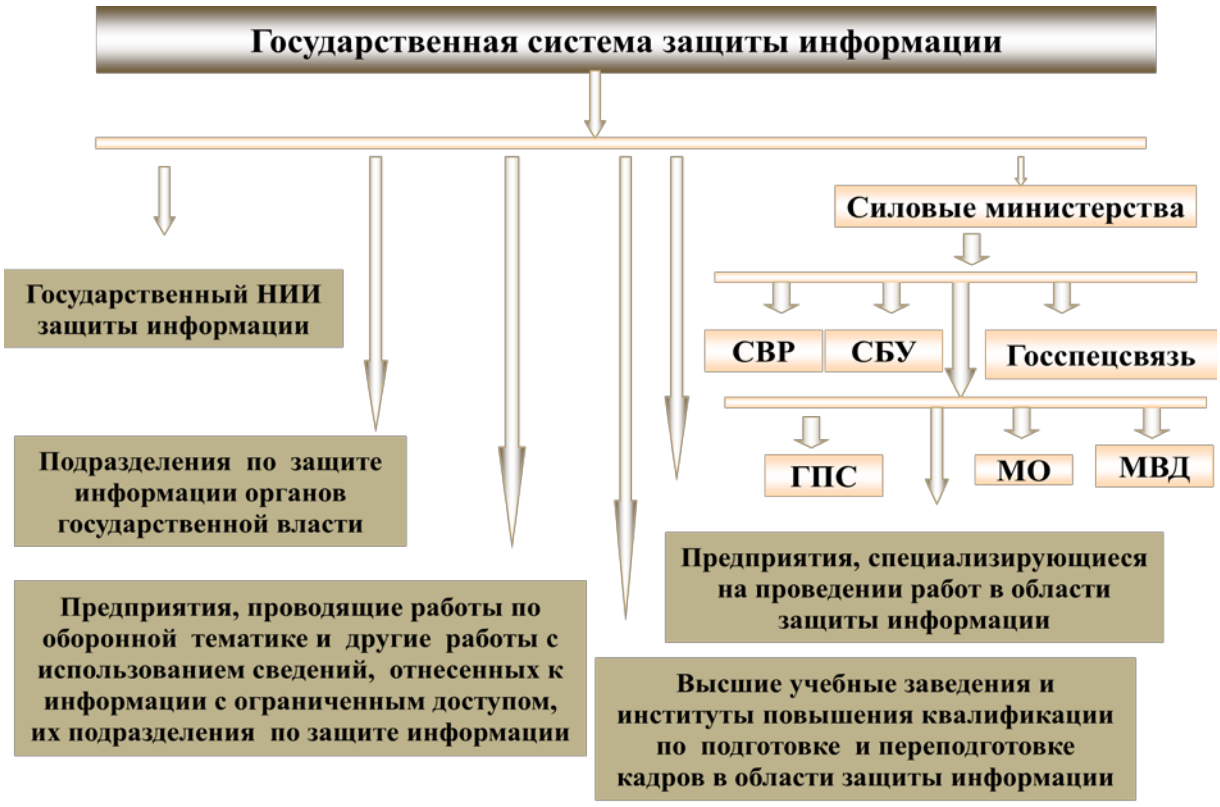

Рис. 10. Система защиты информации в Украине

Она позволяет решать практически весь комплекс задач по защите информации на объектах информационной деятельности и в ИКС государственных органов, предприятий, учреждений и организаций.

Обязательным условием обеспечения защиты информации, которая циркулирует в ИКС и на объектах информационной деятельности, является получение объективной оценки уровня защищенности информации. Это осуществляется через систему государственной экспертизы и аттестации.

Эффективность работ по технической защите информации может быть достигнута при условии применения защищенных средств обработки информации и средств ее защиты, которые имеют соответствующие сертификаты и экспертные выводы. Для этого средства, которые поступают на украинский рынок и потребители которых принадлежат к сфере государственного управления, проходят проверку на соответствие требованиям технической защиты информации в Украинской государственной системе сертификации продукции УКРСЕПРО, а также через государственную экспертизу в сфере технической защиты информации.

В Украине создана система подготовки, переподготовки и повышения квалификации специалистов по защите информации. В этой системе сформирована структура необходимых специальностей и специализаций, которая осуществляется в 20 высших учебных заведениях (в том числе в Государственном университете телекоммуникаций). Обеспечивается разработка методических основ научно обоснованной системы подготовки специалистов по защите информации.

Сегодня среди основных работ, которые проводятся для обеспечения последующего развития систем технической защиты информации, можно отметить работы по:

- определению путей упорядочения и оптимизации мероприятий по созданию, экспертизе и внедрению в эксплуатацию ИКС государственных органов и учреждений, в первую очередь, предназначенных для обработки секретной информации;
- повышению безопасности отечественных информационных ресурсов путем разработки и внедрения в автоматизированных системах государственных органов и учреждений отечественной защищенной ОС;
- разработке современных нормативных документов по защите информации от утечки по техническим каналам, созданию и внедрению комплексов технической защиты информации на объектах информационной деятельности.

Государственный университет телекоммуникацийпринимает активное участие в этом процессе. Он является коллективным членом технического комитета стандартизации ТК 107 "Техническая защита информации" (рис. 11).

Рис. 11. Технический комитет стандартизации

На ТК 107 возлагаются функции разработки, рассмотрения и согласования международных (региональных) и национальных стандартов в закрепленной сфере деятельности, участие в работе родственных ТК международных и региональных организаций и формирование позиции Украины по разрабатываемым нормативным документам этих организаций.

Комитет состоит из трех подкомитетов, которые в точности соответствуют направлениям деятельности кафедр университета, входящих в учебно-научный институт защиты информации.

Заключение

Решение вопросов защиты данных в современных информационных системах будет успешным только при условии использования комплексного подхода к построению системы обеспечения безопасности информации.

Важную роль в создании комплексного подхода к построению системы обеспечения безопасности информации непосредственно играют принципы и этапы разработки СЗИ.

На сегодня в Украине создана соответствующая нормативно-правовая база, которая определяет основные принципы технической защиты информации, нормы и требования по

технической защите информации, порядок проведения работ и осуществления контроля его эффективности.

Обязательным условием обеспечения защиты информации, которая циркулирует в ИКС и на объектах информационной деятельности, является получение объективной оценки уровня защищенности информации.

Эффект повышения безопасности информационных систем заключается: в увеличении роста ВВП, международной торговли страны, экспорта, производительности труда граждан, числа рабочих мест, добавленной стоимости в год.

Литература

1. Торокин А.А. Основы инженерно-технической защиты информации (Книга 1. Угрозы безопасности информации) – М.: РГГУ, 2005. – 266 с.

2. Варлатая С.К., Шаханова М.В. Аппаратно-программные средства и методы защиты информации: Учебн. пособие.–Владивосток: ДВГТУ, 2007. –318 с.

3. Железняк В.К. Защита информации от утечки по техническим каналам: Учебн. пособие.–СПб.: ГУАП, 2006. – 188 с.

4. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия–Телеком, 2014.– 586 с.

5. Малюк А.А. Защита информации в информационном обществе: Учебн. пособие.– М.: Горячая линия–Телеком, 2015.– 230 с.

6. Михайлов Ю.Б. Научно-методические основы обеспечения безопасности защищаемых объектов. – М.: Горячая линия–Телеком, 2015.– 322 с.

7. Положення про технічний захист інформації в Україні. – 27 вереоня 1999 р.№1229/99, поточна редакція від 04.05.2008, підстава 333/2008.

Надійшла 29.10.2015 р. Рецензент: д.т.н., проф. Шевченко В.Л.