УДК 004.056:061.68

М.А. Колтик

ПРОБЛЕМЫ МАССОВОГО ПОСТРОЕНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ (КСЗИ) И ПУТИ ИХ РЕШЕНИЯ

Рассматривается феномен КСЗИ, цели, задачи и принципы его построения. Проводится анализ некоторых способов проведения испытаний и аудита КСЗИ, а также проблем, которые при этом возникают. Предлагается использование программных средств автоматизированной поддержки проведения испытаний и аудита КСЗИ как один из методов их преодоления.

Введение

Принятие решений во всех сферах жизнедеятельности предприятия или организации все в большей степени базируется на информационных процессах. Анализ этих процессов с последующей выработкой управляющих решений осуществляется на основе информационных моделей, построенных на современных информационно-телекоммуникационных технологиях. Поэтому защита информации представляет собой самостоятельную составляющую безопасности предприятия в целом, значение которой с каждым годом растет.

Информационный ресурс становится одним из главных источников экономической эффективности предприятия. Фактически наблюдается тенденция, когда все сферы жизнедеятельности предприятия становятся зависимыми вот информационного развития, в процессе которого они сами порождают информацию и сами же ее потребляют.

Степень автоматизации фирмы определяет зачастую ее конкурентоспособность и при этом является источником многочисленных угроз безопасности.

На современном этапе развития основными угрозами безопасности предприятия являются угрозы в сфере информационного обеспечения. Последствиями успешного проведения информационных атак могут быть компрометация или искажение конфиденциальной информации, навязывание ложной информации, нарушение установленного регламента сбора, обработки и передачи информации, отказы и сбои в работе технических систем, вызванные преднамеренными и непреднамеренными действиями, как со стороны конкурентов, так и со стороны преступных сообществ, организаций и групп.

В сознании многих людей защита информации это, прежде всего, защита информации в компьютерных системах от несанкционированного доступа, осуществляемая техническими средствами защиты. Конечно, эта точка зрения неверна точно так же, как неверна и точка зрения другой полярности: все определяется организационно-режимными мерами. Надежное обеспечение безопасности информации немыслимо без реализации комплексного подхода к решению этой задачи.

Отсюда и потребность как в создании комплексной системы защиты информации (КСЗИ) на предприятии, так и в проведении испытаний и оценки ее эффективности, подготовке специалистов по данному профилю.

Цель данной работы – анализ проблем, которые связаны с массовым построением КСЗИ и рассмотрение автоматизации как одного из возможных путей их решения.

Рассматриваются проблемы, связанные с проведением испытаний и аудита КСЗИ. Данные проблемы, также, анализируются в работах Ю. Барсуковского, Д. Замятина, М. Прокофьева и других. Однако проблема актуальности использования программных средств автоматизированной поддержки при проведении испытаний и аудита КСЗИ в Украине, является перспективной и не достаточно изученной.

Цель, задачи и принципы построения КСЗИ

КСЗИ представляет собой совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации предприятия [1].

Под КСЗИ также понимают совокупность организационных и инженерно-технических мероприятий, которые направлены на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа.

Организационные мероприятия являются обязательной составляющей любой комплексной системы защиты информации. Инженерно-технические мероприятия проводятся в случае необходимости.

Данные организационные мероприятия включают создание концепции информационной безопасности, а также:

- создание должностных инструкций для пользователей и обслуживающего персонала;
- создание правил администрирования компонент информационной системы, учета, сохранения, размножения, удаления носителей информации, идентификации пользователей;
- разработку планов действий в случае выявления попыток несанкционированного доступа к информационным ресурсам системы, выхода из строя средств защиты, возникновения чрезвычайной ситуации;
- обучение правилам информационной безопасности пользователей.

В случае необходимости, в рамках проведения организационных мероприятий может быть создана служба информационной защиты, режимно-пропускной отдел, проведена реорганизация системы делопроизводства и сохранения документов.

Инженерно-технические мероприятия это совокупность специальных технических средств и их использование для защиты информации. Выбор инженерно-технических мероприятий зависит от уровня защищенности информации, который необходимо обеспечить.

Инженерно-технические мероприятия, которые проводятся для защиты информационной инфраструктуры организации, могут заключаться в использовании защищенных подключений, межсетевых экранов, распределении протоколов между сегментами сети, использовании средств шифрования и защиты от несанкционированного доступа.

В случае необходимости, в рамках проведения инженерно-технических мероприятий, может использоваться установление в помещениях систем охранно-пожарной сигнализации, систем контроля и управления доступом.

Отдельные помещения могут быть оснащены средствами защиты от утечки акустической (речевой) информации [2].

Основной целью КСЗИ является обеспечение непрерывности бизнеса, устойчивого функционирования предприятия и предотвращения угроз его безопасности.

КСЗИ направлена на:

1) защиту законных интересов организации от противоправных посягательств;

2) недопущение:

- хищения финансовых и материально-технических средств;
- уничтожения имущества и ценностей;
- разглашения, утечки и несанкционированного доступа к служебной информации;
- нарушения работы технических средств обеспечения производственной деятельности, включая информационные технологии.

Исходя из целей КСЗИ, можно определить стоящие перед ней задачи. К ним относятся:

1) прогнозирование, своевременное выявление и устранение угроз безопасности персонала и ресурсам коммерческого предприятия, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

2) отнесение информации к категории ограниченного доступа (служебной и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), отнесение ресурсов к различным уровням уязвимости (опасности), подлежащих сохранению;

3) создание механизма и условий оперативного реагирования на угрозы безопасности, проявления негативных тенденций в функционировании предприятия;

4) эффективное пресечение угроз со стороны персонала, его посягательств на ресурсы, на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;

5) создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния, последствий нарушения безопасности предприятия.

Обеспечение безопасности предприятия должно основываться на следующих основных принципах:

- системности;
- комплексности;
- своевременности;
- непрерывности защиты;
- разумной достаточности;
- гибкости;
- специализации;
- взаимодействии и координации (должно осуществляться планирование);
- совершенствовании;
- активности;
- экономической эффективности;
- простоты применяемых защитных мер и средств.

Рассмотрим некоторые принципы построения КСЗИ подробнее.

Принцип системности требует применения системного подхода в качестве методологической базы при анализе комплексной системы защиты информации. Основная цель системного подхода – формализация вербальных описаний и составление алгоритма деятельности. Суть его заключается в том, чтобы при оценке эффективности мероприятий безопасности не ограничиваться рассмотрением только самой системы, но и учитывать влияния на нее внешних факторов. Применение системного подхода при разработке технологий управления безопасностью позволяет реализовать синергетический эффект, являющийся результатом упорядочивания организационных структур управления, взаимодействия, кооперации и интеграции с другими подсистемами анализируемой системы, устранения ненужных процедур, а в итоге – результатом достижения равновесного состояния функционирования системы.

Системный подход при построении КСЗИ предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности предприятия.

При создании системы защиты необходимо учитывать все слабые, наиболее уязвимые места предприятия, а также характер, возможные объекты и направления атак на автоматизированную систему (АС) предприятия со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения и несанкционированного доступа (НСД) к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Принцип комплексности предполагает, что система защиты предприятия должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности персонала, материальных и финансовых средств от возможных угроз всеми доступными законными средствами, методами и мероприятиями. Принцип комплексности позволяет оценить, в целом, главные вопросы защиты: что защищается, кто защищает и как защищается?

В распоряжении специалистов по безопасности имеется широкий спектр мер, методов и средств защиты.

Комплексность системы защиты информации достигается охватом всех возможных угроз и согласованием между собой разнородных методов и средств, обеспечивающих защиту всех элементов предприятия.

Защита должна строиться эшелонировано. Внешняя защита обеспечивается физическими средствами, организационными и правовыми мерами. Прикладной уровень защиты, учитывающий особенности предметной области, образует внутренний рубеж обороны. Да, одной из наиболее укрепленных линий обороны должны быть средства защиты в автоматизированных системах.

Принцип своевременности означает, что меры защиты не должны «запаздывать». Например, бесполезно выводить охранную сигнализацию на пульт дежурного, который сможет прибыть в случае тревоги на объект охраны лишь спустя полчаса.

Принцип непрерывности. В настоящее время общепринятым является процессный подход к обеспечению безопасности информации. Защита информации – это не совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла систем предприятия, начиная с самых ранних стадий проектирования, а не только на этапе их эксплуатации.

Во многих зарубежных стандартах, зафиксирована циклическая схема процесса обеспечения безопасности информации обозначаемая как PDCA (англ. Plan-Do-Check-Act). Кроме того, принцип непрерывности подчеркивает недопустимость перерывов в работе средств защиты, устанавливая повышенные требования к их надежности.

Принцип разумной достаточности учитывает тот факт, что создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту, поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Часто приходится создавать систему защиты в условиях большой неопределенности, поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Естественно, что для обеспечения возможности варьирования уровня защищенности средства защиты должны обладать определенной гибкостью. Особенно важно это свойство в тех случаях, когда средства защиты необходимо устанавливать на работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости спасает владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Принцип простоты применения состоит в том, что механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не следует требовать от пользователя выполнения рутинных малопонятных эму операций (ввод нескольких паролей и имен и т. д.).

Важнейшими условиями обеспечения безопасности являются законность, достаточность, соблюдение баланса интересов личности и предприятия, высокий профессионализм представителей службы безопасности, подготовка пользователей средств вычислительной техники и соблюдение ими всех установленных правил сохранения конфиденциальности, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами.

Обеспечение информационной безопасности, для все большего количества государственных предприятий, частных компаний и отдельных лиц, является центральной проблемой, которая нуждается в решении и стимулирует массовую заинтересованность в проектировании и разработке КСЗИ для отдельных компаний.

В процессе построения КСЗИ, согласно требований нормативных документов, ее последовательность должна включать один и тот же набор этапов независимо от того, создается ли КСЗИ для автоматизированной системы, которая уже существовала до этого момента или осуществляется построение КСЗИ одновременно с проектированием новой автоматизированной системы. Некоторые второстепенные этапы работ могут быть исключены или совмещены с более крупными, если это способствует эффективности процесса построения КСЗИ, но ни в коем случае не приводит к ухудшению качества разрабатываемой системы защиты.

Для компаний, разрабатывающих и внедряющих в своих автоматизированных системах КСЗИ, возникает проблема проведения испытаний, оценки эффективности и сертификации в соответствии с необходимыми стандартами (корпоративными, государственными, международными).

Для проведения данных работ целесообразно привлекать специализированные компании, которые имеют большой опыт и штат профессионалов в отрасли обеспечения и контроля состояния информационной безопасности. Кроме этого, они обеспечивают установление оборудования и специализированного программного обеспечения, а также проводят его обновление и отслеживают общий уровень системы информационной безопасности [3].

Такой подход является альтернативой для создания собственной постоянно действующей службы защиты информации на предприятии, проведения ряда организационных и технических мероприятий по обеспечению ее функционирования. Он позволяет решить много проблем, как с финансовой точки зрения, так и организационной.

Методы и средства проведения испытаний и аудита КСЗИ

В процессе проведения испытаний КСЗИ различных автоматизированных систем, а также оценки их качественных и количественных характеристик, используются достаточно разные методы и средства.

Проведение активного аудита. Широко используется метод активного аудита или тесты на преодоление защиты. Задача заключается в том, чтобы преодолеть принятую на предприятии информационную систему безопасности. Тесты касаются, в первую очередь, технической защиты информации. Фирма консультант выступает в роли преступника (внутреннего или внешнего), задача которого скомпрометировать корпоративную систему заказчика, получить конфиденциальные данные или нарушить функционирование системы. Основными целями данных попыток является констатация и доказательство возможности взлома системы, а также выявление реакции персонала на атаку (как администраторов, так и обычного персонала).

В основе данного метода лежат изложенные ниже принципы.

Первый принцип – наличие четкого описания модели нарушителя, в рамках которой действуют аудиторы. Рассматриваются отдельно внутренний нарушитель (например, сотрудник компании) и внешний нарушитель (например, хакер, действующий через Интернет). Уровень квалификации нарушителя считается достаточным для выполнения сложных задач по проникновению в информационную систему. Это автоматически означает, что квалификация самих аудиторов должна соответствовать данному уровню.

Второй принцип – уточнение области проведения аудита непосредственно в процессе работы на объекте. На практике заказчик часто предоставляет ограниченный набор сведений об информационной системе (что происходит, когда информационная система развивалась непланомерно и, как следствие, плохо документировалась), а аудиторы проводят инвентаризацию ресурсов информационной системы.

Это позволяет выявить «потерянные» ресурсы (и в большинстве случаев плохо защищенные), что особенно актуально для крупных корпоративных информационных систем.

Третий принцип – аудитор изначально имеет только физический доступ к обследуемой информационной системе, логические права доступа (аутентификационные данные) ему не предоставляются (за редким исключением). Далее аудитор отрабатывает все возможные пути повышения привилегий от «нулевого» уровня, оценивая критичность и вероятность их реализации.

Четвертый принцип – анализ путей повышения привилегий. С одной стороны, например, наличие уязвимости в программном обеспечении автоматически не приводит к нарушению безопасности, так как многие уязвимости могут быть успешно реализованы только при определенном сочетании факторов. С другой стороны, использование штатных возможностей (именно возможностей, а не ошибок программного обеспечения или конфигурации) информационной системы в определенной комбинации может привести к нарушению информационной безопасности. Выявление таких ситуаций невозможно без применения творческого, неформального подхода к анализу защищенности.

Пятый принцип – анализ влияния выявленных в ходе активного аудита уязвимостей на защищенность всей информационной системы в целом. Данный принцип заключается в следующем: не столь важно, какая именно уязвимость была обнаружена, важно то, как наличие той или иной уязвимости влияет на защищенность всей информационной системы, насколько вся система устойчива к уязвимостям. Другими словами, в ходе аудита проводится анализ архитектуры безопасности информационной системы.

Шестой принцип – поиск новых уязвимостей (не зафиксированных в различных базах уязвимостей, таких как CVE, OSVDB и т.п.) непосредственно в ходе работы на объекте в режиме реального времени.

Седьмой принцип – строгая система классификации уязвимостей. Каждая выявленная в ходе аудита уязвимость оценивается (по шкале с простыми и понятными описаниями уровней) с точки зрения её критичности, простоты и вероятности её реализации. Эти данные в дальнейшем используются для проведения анализа информационных рисков.

Восьмой принцип – отказ от приоритетного использования сканеров уязвимостей. Подобный инструментарий используется только на этапе предварительного сбора информации для автоматизации рутинной работы. Существенным недостатком сканеров является большое количество ложных срабатываний и невозможность обнаружения уязвимостей, отсутствующих в базе сканера (например, недавно появившихся уязвимостей, большого числа локальных уязвимостей, нетривиальных ошибок конфигурации).

Девятый принцип – применение методов социальной инженерии для имитации действий нарушителя информационной безопасности, направленных на пользователей информационной системы компании. Эти методы позволяют оценить уровень квалификации пользователей в области обеспечения информационной безопасности и вероятность реализации атак, выполняемых нетехническими способами [4].

Успешная реализация атаки – действенное средство доказать руководству компании необходимость увеличения затрат на обеспечение информационной безопасности, особенно, если в результате успешного взлома фирме-эксперту удалось незаконно получить какую-либо конфиденциальную информацию руководства. Кроме того, тест на преодоление защиты является хорошим способом проверить соблюдение персоналом принятой политики безопасности, например, правил хранения и смены пароля.

Недостатком данного метода является отсутствие в результате целостной картины состояния информационной безопасности. Заказчик лишь получает информацию о том, что исследуемая система уязвима. Проведение определенной атаки

не позволяет выявить весь спектр слабых мест системы и тем более не дает никаких рекомендаций по повышению уровня защищенности автоматизированной системы.

Своеобразным недостатком данного метода является то, что его успешное проведение невозможно без привлечения высококвалифицированных аудиторов информационной безопасности, обладающих творческим подходом к анализу защищенности информационных систем и опытом в области проведения тестов на проникновение [4].

Проведение аудита на соответствие стандартам. Под аудитом подразумевается оценка текущего состояния КСЗИ компьютерной системы на соответствие некоему стандарту или предъявленным требованиям. Стандарты могут быть внутрикорпоративными или общими (как государственными, так и коммерческими).

В большинстве случаев аудит КСЗИ требуется, когда автоматизированная система предназначена для обработки конфиденциальной или секретной информации. Для каждой категории информации стандартами определяется нижняя граница уровня безопасности автоматизированной системы.

Проведение аудита полезно также после построения автоматизированной системы и ее подсистем безопасности на этапе приемки в эксплуатацию – для оценки степени соблюдения предъявляемых к ней требований. Следует отметить, что аудит автоматизированной системы рекомендуется проводить периодически (например, раз в год), так как состояние любой системы изменяется с течением времени и к моменту очередного аудита она может не иметь ничего общего с тем, что было зафиксировано при предыдущем аудите.

Отчет об аудите содержит оценку соответствия системы данному стандарту, но не содержит рекомендаций и предложений по устранению выявленных уязвимых мест и повышению уровня защищенности [3].

Проведение экспертного аудита или обследование. Экспертный аудит можно условно представить как сравнение состояния информационной безопасности с «идеальным» описанием, которое базируется на требованиях, которые были предъявлены руководством в процессе проведения аудита или описании «идеальной» системы безопасности, основанное на аккумулированном в компании – аудиторе мировом и частном опыте [5].

Оценка автоматизированной системы – наиболее сложный и полезный вид работ по обеспечению информационной безопасности. В рамках этой работы фирма-эксперт проводит комплексную оценку автоматизированной системы с учетом ее особенностей.

Такая оценка включает анализ информационных потоков аппаратного и программного обеспечения, сетевой инфраструктуры, методов управления и администрирования компонентов.

После сбора и упорядочивания информации специалисты фирмы-эксперта проводят анализ состояния информационной безопасности, состоящей из нескольких этапов:

- анализ существующей организационной структуры обеспечения информационной безопасности, в том числе анализ функций службы информационной безопасности;
- анализ взаимоотношений подразделений по вопросам обеспечения защиты информации, вопросов подчиненности и структуры службы информационной безопасности;
- анализ существующей нормативно-правовой базы информационной безопасности автоматизированной системы, в том числе оценка принятой политики безопасности, организационно-распорядительных документов, положений и инструкций по обеспечению защиты информации, а также анализ их соответствия существующим законодательным и нормативным актам;
- анализ мер технической защиты информации, в том числе анализ существующих мер и средств технической защиты информации, а также порядка их применения;
- рассмотрение и анализ используемых заказчиком средств разграничения доступа и защиты вот несанкционирован-

ного доступа (в частности, при работе с Интернет), антивирусных средств, межсетевых экранов, защиты с помощью паролей, системы обнаружения вторжений, криптографических средств защиты информации, методов контроля целостности и т. д.;

- анализируют порядок использования встроенных механизмов защиты компонентов в автоматизированной системе;
- оценивают достаточность мер и правильность использования средств технической защиты информации;
- производят выявление угроз безопасности (как внутренних, так и внешних) и определяют существующие уязвимые места в компонентах автоматизированной системы;
- производят оценку рисков для автоматизированной системы;
- ранжируют угрозы по вероятности их возникновения в данной автоматизированной системе и мере возможного ущерба вот реализации угроз.

В результате фирма-эксперт предоставляет:

- список наиболее опасных угроз безопасности;
- перечень и описание уязвимых мест компонентов, включая описание их источников (модель нарушителя) и механизмов их реализации;
- рекомендации по доработке существующей системы защиты информации компании.

Рекомендации фирмы-эксперта могут касаться совершенствования организационно-штатной структуры, доработки и создания нормативных документов, положений и инструкций по обеспечению информационной безопасности.

Кроме того, эксперты могут дать рекомендации по применению штатных средств защиты компонентов, а также использованию дополнительных средств защиты информации и методов контроля и аудита состояния информационной безопасности [3].

Исходя из характеристики вышеописанных методов оценки защищенности автоматизированных систем, следует отметить, что каждый из них имеет преимущества и недостатки, а их применение зависит от поставленной задачи компанией заказчиком перед экспертами.

В условиях постоянно возрастающего значения автоматизации и использования информационных технологий на предприятиях, увеличения количества угроз для автоматизированных систем, реализация которых приводит к финансовым и имиджевым потерям компаний, возрастает и потребность в защите персональных данных, корпоративной и государственной информации. В свою очередь, увеличивается потребность в проектировании и разработках КСЗИ для различных автоматизированных систем и соответственно проведении их испытаний, аудита, подтверждения соответствия различным стандартам (корпоративным, государственным, международным).

Увеличение количества разработанных и внедренных КСЗИ, повышает количество необходимых оценок и экспертиз на предмет их соответствия государственным стандартам Украины.

Проблемы, связанные с проведением испытаний и аудита КСЗИ и возможные пути их решения

Проведение различных экспертиз традиционными методами связано с целым рядом трудностей, как экономического, так и психологического характера [6].

Учитывая то, что при проведении анализа информационной защищенности автоматизированных систем необходимо брать во внимание большое количество не связанных между собой факторов, в процессе роботы увеличивается вероятность допущения ошибок.

Также, увеличивает вероятность допущения ошибок, большое количество рутинных операций, которые проводятся экспертами во время аудита системы.

Необходимость в массовом построении КСЗИ, в чем в настоящий момент нуждается все больше компаний отечественного рынка, также, порождает проблему, которая связана с необходимостью привлечения к работе достаточно большого количества специалистов в сфере защиты информации. Их подготовка требует больших затрат государства или компании, которая проводит переподготовку своих работников. К тому же подготовка квалифицированного работника занимает достаточно много времени.

Также, увеличение количества работников, которые задействованы со стороны компании-эксперта, при проведении экспертиз, является более экономически затратным шагом, а также повышает вероятность возникновения ошибок при проведении обследований и экспертных оценок КСЗИ.

Еще одной проблемой является то, что разработкой, построением, оценкой и сопровождением КСЗИ могут заниматься только организации, которые имеют лицензию на проведение соответствующих работ, которые касаются сферы защиты информации. Это условие ограничивает перечень организаций, которые могут проводить данные работы. Поэтому данное условие, с одной стороны отвечает международной практике лицензирования организаций, которые проводят ограниченный перечень работ, а с другой стороны требуют от организации и ее работников дополнительных усилий, которые должны быть направлены на получение государственной лицензии, на право проведения данных работ.

Данные проблемы подталкивают организации, проводящие экспертизу различных автоматизированных систем к поиску их решений. И одним из таких решений является разработка и использование при проведении испытаний КСЗИ автоматизированных средств поддержки.

Их внедрение способствует оптимизации расходов и полученных результатов при разработке проекта.

Для облегчения реализации поставленных задач, повышения качества выполняемых работ, уменьшения рабочей нагрузки на специалистов, особенно молодых, которые не имеют достаточного опыта работы, также целесообразно использовать средства автоматизированной поддержки.

Использование специальных программных средств позволит сократить время на реализацию проекта, поможет недостаточно опытным работникам проводить работы, которые нуждаются в их большей квалификации и опыте.

Разработка и использование программных средств автоматизированной поддержки проведения испытаний КСЗИ позволяет оптимизировать количество работников, которые разрабатывают проект, а также задействовать менее квалифицированный персонал (при условии их обучения использованию программного обеспечения), эффективно руководить процессом реализации проекта, оперативно исправлять проблемы, которые появились и негативные тенденции.

Использование средств автоматизированной поддержки проведения испытаний КСЗИ должно облегчать решение отдельных поставленных перед экспертом задач. В этом большую роль играет простота и понятность при работе специалиста с новым программным обеспечением. Время на обучение специалиста работе с новой программой должно занимать сравнительно небольшое время. При разработке подобного программного обеспечения необходимо помнить основную цель его внедрения, а именно повышение эффективности работы специалиста и снижение затрат предприятия, которые могут измеряться как в денежном, так и временном эквиваленте, что, несомненно, является ключевой задачей в любой компании. Использование программного обеспечения автоматизированной поддержки проведения испытаний КСЗИ является, бесспорно, конкурентным преимуществом любого предприятия.

Выводы

Использование специализированного программного обеспечения, которое применяется при проведении испытаний или сертификации КСЗИ должно быть целесообразным. Его использование, без

сомнения, не сможет полностью заменить работника, но может значительно облегчить его труд, сократить потраченное время на выполнение рутинных процедур. Программный продукт может выступать определенным сконцентрированным опытом предыдущих проектов, которые были реализованы ранее. Автоматизация позволит сокращать время, потраченное компанией на разработку и реализацию отдельного проекта, уменьшать количество задействованных работников, а также позволит привлекать работников с не большим опытом работы, к тем проектам, которые нуждаются в высококвалифицированных специалистах и соответственно повышать качество выполняемых работ.

Проблема возможных перспектив разработки и использования программных средств автоматизированной поддержки проведения испытаний КСЗИ является актуальной и требует дальнейшего исследования, в части анализа подходов, методов и средств для реализации данного программного продукта.

1. *Грибунин В.Г.* Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений / В.Г. Грибунин В.В. Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.
2. *Грайворонський М.В. Новіков О.М.* Безпека інформаційно-комунікаційних систем: Підручник для вузів. – К.; 2007. – 1005 с.
3. *Барсуковский Ю.* Аудит систем информационной безопасности – проблемы и решения // Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине. – К.: НТУ Украины “КПИ”. – 2002. – Вып. 4. – С. 29 – 33.
4. http://www.dsec.ru/about/articles/active_audit/
5. http://www.bezpeka.com/ru/lib/sec/analys/art526.html
6. *Замятин Д., Прокофьев М.* Алгоритмические особенности экспертных систем, ориентированных на проблемы защиты информации // Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине. – Киев: НТУ Украины “КПИ”. – 2000. – Вып. 1. – С. 252 – 253.

Получено 30.05.2011

Об авторе:

Колтик Максим Анатолиевич,
аспирант.

Место работы автора:

Институт программных систем
НАН Украины.
03187, Киев-187,
проспект Академика Глушкова, 40.
Тел.: 067 218 2809
E-mail: maxfaktor@ua.fm