УДК: 004.056.53

Толюпа С. В., доктор техн. наук, проф. Тел.. +38(050)773 46 57. E-mail : tolupa@i.ua
Наконечный В. С. доктор техн. наук. Тел.+380 (66) 305 15 85. E-mail: nvc2006@mail.ru
Якименко Ю. М., канд. военных наук. Тел.+380(67) 277 22 20. E-mail: yakimenko.um@mail.ru
(Государственный университет телекоммуникаций, г. Киев)

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Tolyupa S. V., Nakonechnyy V. S., Yakymenko Yu. M. The information security in automated information systems. The article analyzes the problems of information protection in automated systems of information processing and concludes that to date there is no effective approach to their solution. There is clarified the structure of the information security system and its functions, allowing to approach the solution to the problem of protection from system positions. The security system information can be represented in the form of subsystems: computer security, data security, secure software, secure communications. Offers Cisco with the aim of increasing the effectiveness of information security can be recommended for implementation in the organization.

***Keywords*:** security, information, automated information system, information protection system, threat, ACS

Толюпа С. В., Наконечний В. С., Якименко Ю. М. Забезпечення безпеки інформації в автоматизованих інформаційних системах. Проведено аналіз проблем захисту інформації в автоматизованих системах обробки інформації і зроблено висновок про те, що на сьогоднішній день відсутній ефективний підхід до їх вирішення. Уточнено структуру системи захисту інформації та її функції, що дозволило підійти до вирішення проблеми захисту з системних позицій. Систему забезпечення безпеки інформації можна уявити у вигляді підсистем: комп'ютерна безпека, безпека даних, безпечне програмне забезпечення, безпека комунікацій. Пропозиції компанії Cisco з метою підвищення ефективності інформаційної безпеки можуть бути рекомендовані до впровадження в організації

***Ключові слова*:** безпека, інформація, автоматизована інформаційна система, система захисту інформації, загроза, АСУ.

Толюпа С. В., Наконечный В. С., Якименко Ю. М. Обеспечение безопасности информации в автоматизированных информационных системах. Проведен анализ проблем защиты информации в автоматизированных системах обработки информации и сделан вывод о том, что на сегодняшний день отсутствует эффективный подход к их решению. Уточнена структура системы защиты информации и её функции, что позволило подойти к решению проблемы защиты с системных позиций. Систему обеспечения безопасности информации можно представить в виде подсистем: компьютерная безопасность, безопасность данных, безопасное программное обеспечение, безопасность коммуникаций. Предложения компании Cisco с целью повышения эффективности информационной безопасности могут быть рекомендованы к внедрению в организации.

***Ключевые слова*:** безопасность, информация, автоматизированная информационная система, система защиты информации, угроза, АСУ.

1. Введение и постановка задачи. Задачи создания и исследования процессов функционирования, совершенствования и развития систем защиты информации (СЗИ) в той или иной степени нашли отражение в трудах ряда отечественных и зарубежных ученых. Однако, до настоящего времени они в полной мере не изучены. Остаются дискуссионными методологические, методические и практические аспекты исследования эффективности сложных систем, таких, как автоматизированные системы (АС), которые представляют собой среду обработки информации, а также информационных ресурсов в информационно-телекоммуникационных системах. В подтверждение выше приведенного АС можно рассматривать как автоматизированную информационную систему (АИС).

Важность и сложность проблемы защиты информации в автоматизированных системах обработки информации требует принятия кардинальных мер в выработке рациональных решений, для чего необходимо сконцентрировать усилия на вопросах разработки общей концепции защиты интересов всех субъектов информационных отношений с учетом особенностей тех прикладных областей, в которых функционируют различные АИС.

Анализ литературных данных. В современных условиях наиболее перспективным способом проверки достигнутого качества функционирования и уровня защищенности информации в автоматизированных системах, как отмечается в [1], является процедура её оценки по выполнению требований информационной безопасности (ИБ).

В настоящее время действуют два относительно самостоятельных направления решения этой проблемы. Первое направление связано с защитой средств вычислительной техники (СВТ), второе – с защитой АС. Как показывает практика, при рассмотрении вопросов защиты СВТ ограничиваются только программно-техническими аспектами функционирования системы, в то время как для защиты АС рассматриваются организационные меры защиты (вопросы физического доступа, защиты информации от утечки по техническим каналам и другие) [2]. При таком подходе СВТ представляют собой программно-технические средства, а АС включает в себя СВТ, обслуживающий персонал и систему организационных мероприятий, обеспечивающих ее функционирование, а также помещения, пользовательскую информацию, бумажную документацию и так далее. Объединение двух самостоятельных направлений для оценки уровня защищенности АИС также остаётся нерешённой проблемой.

В работе Маслова Н. А. [3] приводятся различные схемы построения защиты информации, в том числе и модель адаптивного управления безопасностью, раскрывается способ оценки эффективности адаптивной системы защиты информации путём *оптимизационного или комбинаторного подхода.* Однако для детальной проработки их возможностей требуется проведение дополнительных технических экспертиз с учётом специфики предназначения АИС.

Цель и задачи исследования. Переход к новым формам государственного и хозяйственного управления экономикой в Украине, в условиях дефицита и противоречивости правовой базы, породил целый комплекс проблем в области защиты данных, информации, знаний и самих информационно-коммуникационных технологий. С появлением и широким распространением АИС информационная безопасность становится одним из важнейших аспектов интегральной безопасности на всех уровнях — национальном, корпоративном или персональном.

Согласно результатам совместного исследования Института информационной безопасности США и ФБР, каждый год отмечается ущерб от компьютерных преступлений в среднем до миллиарда долларов, что составляет около 40 % за год, и наблюдается его рост даже в условиях увеличения затрат на средства обеспечения безопасности [4].

Поэтому актуальным для автоматизированной информационной системы организации продолжает оставаться защищенность от случайного или преднамеренного вмешательства в нормальный процесс её функционирования. Целью исследования является: рассмотреть состояние существующей системы обеспечения безопасности информации в АИС и предложить рекомендации по повышению эффективности её функционирования.

2. Система защиты информации в АИС и её функции. Безопасность АИС организации достигается, прежде всего, обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов системы [2, 5]. Защита информации в АИС – деятельность, которая направлена на обеспечение безопасности обрабатываемой информации и системы в целом, и позволяет предотвратить или осложнить возможность реализации угроз, а также снизить величину потенциального ущерба в результате реализации угроз. Состояние защищённости информации поддерживается с помощью совокупности программных, аппаратно-программных средств и методов, а также организационных мер при ее вводе, выводе, передаче, обработке и хранении в самой АИС.

Следовательно, систему обеспечения безопасности информации структурно можно представить в виде следующих подсистем (см. Рис.1):

- компьютерная безопасность;
- безопасность данных;
- безопасное программное обеспечение;
- безопасность коммуникаций.

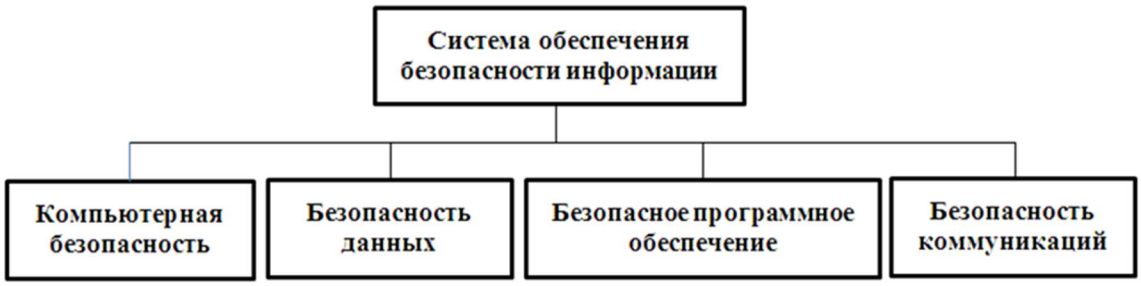

Рис. 1. Система обеспечения безопасности информации в АИС

Подсистемы АИС будут независимы друг от друга, а в комплексе - составлять цельную систему защиты информации. Для службы защиты информации будут упрощены задачи:

- контроля состояния системы защиты информации;
- своевременного и адекватного реагирования на определенные виды угроз информации;
- обновления средств системы защиты информации в короткие сроки.

Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности связанных с ним ресурсов.

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашения.

Безопасное программное обеспечение представляет собой общецелевые и прикладные программы и средства, осуществляющие безопасную обработку данных в системе и безопасно использующие ресурсы системы.

Безопасность коммуникаций обеспечивается посредством аутентификации телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам критичной информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

Вполне обоснованным направлением в сфере безопасности представляется рассмотрение зависимости эффективности защиты от привлекаемых ресурсов. Задача выбора стратегии защиты облегчается, если при меньших затратах удастся обеспечить равную или даже большую эффективность защиты. Очевидны и источники экономии затрат, например, использование более экономичных средств универсального характера, рациональное распределение ресурсов и более совершенные формы управления ими, привлечение интегрированных форм обеспечения безопасности и другие. Указанные источники экономии более всего относятся к *крупным* коммерческим структурам.

Для предприятий *среднего и малого бизнеса* количество таких источников заметно сокращается. Концепция системы безопасности *малых структур* должна строиться на защите лишь от отдельных видов опасности. В противном случае защита может себя не оправдать.

Любая угроза и противодействие ей происходят во времени и характеризуются определенными масштабами. Наилучшим вариантом является противодействие, носящее опережающий характер, то есть когда реакция системы защиты начинается до начала реализации опасности. Основанием для реакции могут быть различные оперативные данные, например: сигналы тревоги раннего оповещения.

Если говорить о тактических вопросах системы безопасности информации в АИС, прежде всего, следует иметь в виду надежность мероприятий защиты. Прежде чем определиться в вопросах тактики, надо помнить, что она должна соответствовать стратегии и опираться на точный количественный и экономически обоснованный анализ [2].

Для АИС *среднего и малого масштаба* такой анализ вполне реален даже без средств автоматизации. Однако необходимо привлечь силы специалистов и экспертов, которые могли бы провести анализ обстановки и свойств защищаемой информации, спрогнозировать возможные модели угроз, изучить рынок существующих методов и средств защиты. Результаты этих мероприятий обеспечили бы оценку системы защиты, а при необходимости – усовершенствовали ее.

Для *крупных ИС* нужен несколько иной подход с более высокими требованиями к эффективности и рентабельности защиты целостности информации в АИС [5]. Под защитой информации может пониматься также деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Эта деятельность в свою очередь предполагает применение специфических средств и методов защиты информации, то есть возникают проблемы разработки эффективных систем её защиты и их совершенствования

3. Использование предложений компании Cisco для повышения эффективности безопасности информации в АИС. Компания Cisco имеет опыт и уже законченные решения по построению и защите сетей автоматизированных систем управления (АСУ), который может быть использован для повышения эффективности безопасности информации в АИС организаций. Так, модель информационной безопасности, разработанная Cisco, ориентированная на широкий спектр различных угроз, позволяет обеспечить мониторинг и контроль АСУ, а также защитить их от несанкционированных вмешательств любого типа на всех направлениях, причем постоянно, в любой момент времени. исполнительные устройства), а также применяемые индустриальные протоколы.

Особенно важно осознавать цели защиты информации в АСУ, отличающиеся от аналогичных задач в корпоративных сетях. Портфель интегрированных решений Cisco выполняет эти задачи, обеспечивая прозрачность и непрерывную защиту от самых изощренных атак. Он позволяет государственным и коммерческим заказчикам и операторам АСУ действовать более быстро и интеллектуально *до атаки, во время атаки и после ее отражения.* И при этом – в полном соответствии с требованиями нормативных и законодательных документов. Портфель интегрированных решений Cisco по реализации требований защиты информации в АИС представлен на Рис. 2 [6].

Помимо предложений на рынке услуг эффективных технических решений по защите АСУ, полностью соответствующих требованиям безопасности, компания Cisco активно участвует и в нормотворческой деятельности по разработке и экспертизе нормативных требований по их защите. Использование предложений компании Cisco с учётом реализации требований защиты информации в АИС должны быть экономически обоснованы экспертами для конкретных организаций.

4. Выводы. Всевозрастающая опасность компьютерной преступности выдвигает комплекс новых задач в автоматизированных информационных системах организаций, связанных с их готовностью к защите своих компонентов и ресурсов. Защита безопасности информации в АИС должна быть непрерывным процессом, целенаправленно осуществляемым со времени введения её в эксплуатацию и во время функционирования, с комплексным применением всех имеющихся средств, методов и мероприятий.

Для повышения эффективности безопасности информации в АИС предлагается использование предложений компании Cisco после экономического обоснования экспертами для конкретных организаций, в зависимости от предназначения и условий деятельности.

Требования	ASA-X / ASA-SM	NGFW	IPS / NGIPS / wIPS	AMP / FireAMP	ISE / TrustSec	ESA	WSA	CTD	AC	VSG / ASAv
Идентификация и аутентификация	+	+	+		+	+	+		+	
Управление доступом	+	+	+	+	+	+	+	+	+	
Ограничение программной среды										
Защита машинных носителей					+					
Регистрация событий безопасности	+	+	+	+	+	+	+	+	+	+
Антивирусная защита				+						
Обнаружение вторжений		+	+	+			+	+		
Анализ защищенности		+			+			+		
Обеспечение целостности		+	+	+		+	+			
Обеспечение доступности	Обеспечивается любым решением компании Cisco, в т.ч. и не относящимся к решениям по информационной безопасности									
Защита среды виртуализации		+	+	+	+			+		+
Защита технических средств										
Защита АСУ ТП	+	+	+	+	+	+	+	+	+	
Безопасная разработка	Обеспечивается с помощью подхода Cisco к безопасной разработке (CSDL)									
Управление обновлениями					+					
Планирование мероприятий										
Обеспечение действий в нештатных ситуациях										
Обучение пользователей										
Анализ угроз и рисков				+						
Управление инцидентами		+	+	+	+			+		
Управление конфигурацией	Обеспечивается системами управления сетью и информационной безопасностью									

Рис. 2. Решения Cisco по реализации требований защиты информации в АИС.

Литература

1. Общее описание процедуры аттестации автоматизированных систем по требованиям информационной безопасности [Електронний ресурс] // – Режим доступу : http://kiev-security.org.ua/box/12/140.shtml ; http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7465/032-Maslova.pdf .

2. Бойченко О. В. Модель корпоративного інформаційного захисту об'єкту інформатизації / О. В. Бойченко, Я. І. Торошанко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2011. – №4(20). – С. 15-19.

3. Маслова Н. А. Принципы адаптации в защите корпоративных систем / Н. А. Маслова, В. В. Шамаев // Донецк: Донецкий НТУ «Штучний інтелект». – 2010. – №4. – 429 с.

4. Безопасность информационных систем [Електронний ресурс] // – Режим доступу : http://intuit.valrkl.ru/course-1312/index.html .

5. Толюпа С. В. Пути обеспечения безопасности электронных хранилищ / С. В. Толюпа, Я. И. Торошанко, А. Ю. Мороко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2012. – №3(23). – С. 17-22.

6. Решения Cisco по защите автоматизированных систем управления технологическими процессами [Електронний ресурс] // – Режим доступу : http://www.cisco.com/assets/global/RU/pdfs/brochures/Podhod-Cisco-po-bezopasnosti-ASU-TP.pdf .

Дата надходження в редакцію: 22.07.2015 р. Рецензент: д.т.н., проф. Г. М. Розорінов