НЕДОСТАТКИ СУЩЕСТВУЮЩИХ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DISADVANTAGES OF EXISTING POLICIES OF INFORMATION SECURITY

A. Marchenko

Summary. The article is devoted to revealing and studying the shortcomings of existing information security policies. During the research it was established that all problems can be divided into two groups: theoretical and practical. As part of practical problems, in turn, it is possible to distinguish, legislative, technical and organizational.

Keywords: information security, politics, problems.

Марченко Андрей Юрьевич
Аспирант, Ростовский Государственный Экономический Университет (РИНХ)
Thevanila@mail.ru

Аннотация. Статья посвящена выявлению и изучению недостатков существующих политик информационной безопасности. В процессе исследования установлено, что все проблемы могут быть поделены на две группы: теоретические и практические. В составе практических проблем, в свою очередь, можно выделить, законодательные, технические и организационные.

Ключевые слова: информационная безопасность, политика, проблемы.

Современный уровень развития общества характеризуется широким внедрением перспективных компьютерных технологий в различных сферах человеческой деятельности. Новые информационные технологии активно внедряются во все сферы деятельности государства. Информационные сети обслуживают и управляют банковскими системами, космическими объектами, контролируют работу атомных электростанций, а также распределяют электроэнергию.

В данном контексте сегодня в мире актуализируется проблема защиты информации и информационного пространства. Ее рассматривают не только на уровне одной страны, но и на саммитах глобальных сообществ и организаций, таких как НАТО, ЕС, Большая восьмерка и т.д. [1]. Данные вопросы подлежат постоянному обновлению, как законодательно, так и программно, ведь от этого зависит безопасность государства, его военные, экономические, социальные и человеческие ресурсы.

Фундаментальные положения системно-концептуального подхода защиты информации основываются на необходимости разработки надежной, полной и непротиворечивой политики информационной безопасности. Основной целью этой политики является обеспечение безопасности информации, то есть минимизация недопустимого риска, связанного с возможностью нанесения ущерба государству, юридическим лицам всех форм собственности и гражданам вследствие незаконного получения информации и ее использования [2].

Вместе с тем, несмотря на пристальное внимание к исследуемым вопросам, в процессах разработки и совершенствования политики информационной безопасности есть еще немало недостаточно изученных аспектов, вызывающих возникновение определенных трудностей и проблем, негативно влияющих на показатели эффективности и надежности функционирования системы безопасности в целом. Указанные обстоятельства обуславливают необходимость идентификации указанных трудностей с целью их устранения и предупреждения дальнейшего возникновения, что в свою очередь подтверждает актуальность выбранной темы исследования.

Следует отметить, что проблема защиты информации является чрезвычайно актуальной в XXI веке, ее исследуют многие зарубежные и отечественные ученые. Тему защиты информационного мирового пространства поднимали в своих работах Ботвиник А., Ворожко В., Гуцалюк М., Климчук С. и другие. Вопросам разработки и функционирования систем защиты информации посвящено значительное количество трудов В.Б. Дудикевича, М.П. Карпинского, А.С. Петрова, В.А. Хорошко и др.

Вместе с тем публикации, в которых затрагиваются вопросы разработки методов и способов оценки защищенности открытой информации, в научной литературе встречается опосредованно, а практическое определение таких оценок фактически возложено на экспертные комиссии. В аспекте информационной политики на указанную проблему обратили внимание Г. Почепцов, С.А. Чукут.

Таким образом, цель статьи заключается в выявлении и проведении анализа проблем существующих политик информационной безопасности.

Рассматривая основополагающие принципы разработки и внедрения политики информационной безопас-

Таблица 1. Информационное законодательство новых стран-членов ЕС [4]

Страна	Закон про доступ к информации		Закон о государственных секретах	
	Название	Дата принятия	Название	Дата принятия
Чехия	Порядок доступа к информации	1999	Акт о классификации информации	1998
Эстония	Акт об общественной информации	2000	Акт о государственных тайнах	1999–2000
Литва	Закон об условиях передачи информации общественности	2000	Закон о государственной тайне	1995
Латвия	Закон о свободе информации	1998	Закон о государственной тайне	1997
Польша	О доступе к информации	2001	Акт о защите информации, которая классифицируется	1999

ности, целесообразно отметить, что комплексная защита информации предусматривает разработку теоретических основ ее защиты, как первой составляющей общей проблемы безопасности; использование специальных правовых, физических, организационных и программно-аппаратных средств, которые должны обеспечивать идентификацию и аутентификацию пользователей, а также распределение полномочий доступа к техническим, информационным ресурсам и сервисам информационных систем, учет попыток несанкционированного доступа [3]. Очевидно, что абсолютно безопасную информационную систему создать невозможно, поэтому эффективная политика информационной безопасности является компромиссным решением.

Учитывая вышеизложенное, представляется, что недостатки существующих политик информационной безопасности можно рассматривать с теоретической и практической точек зрения.

Итак, с теоретической точки зори, по мнению автора, наиболее важны:

1. Отсутствие надлежащих теоретических основ и несовершенство научно-методологического базиса управления информацией в контексте обеспечения информационной безопасности, позволяющие адекватно описывать процессы в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов.
2. Неактуальность научно обоснованных нормативно-методических документов по вопросам обеспечения информационной безопасности на базе исследования и классификации угроз информации и выработки стандартных требований к защите.
3. Недостаточная стандартизация подходов к созданию систем защиты информации и рационализация структур управления защитой на объектовом, региональном и государственном уровнях.

С точки зрения практики можно условно выделить три группы проблем: правовые, технические и организационные. Рассмотрим их более подробно.

Правовые

Несовершенство, а по ряду вопросов отсутствие, правовой базы существенно усложняет разработку политик информационной безопасности. Исходя из того, что система информационной безопасности является подсистемой, входящей в общую систему охраны информации, считаем, что ее правовые проблемы невозможно решать без решения законодательных вопросов общего уровня.

Исследование передового мирового опыта показывает, что для полноценного существования страны в информационном пространстве критически важно иметь достаточно действенную правовую базу. Такие условия необходимо создавать для того, чтобы государства могли защитить свои информационные интересы в любом международном сообществе. Например, анализ нормативно-правового обеспечения новых стран-членов ЕС, свидетельствует об устарелости законодательной базы в сфере защиты информации (см. табл. 1).

Вместе с тем, следует отметить, что законы и подзаконные акты составляют верхний эшелон документов, регламентирующих правоотношения в области разработки политики информационной безопасности. Они могут только концептуально определять некоторые подходы и особенности технологии защиты. Основной же смысл работ и оценки их эффективности должен содержаться в специальной нормативной документации. Наличие комплексной, функционально полной системы документации, регламентирующей все этапы проведения мероприятий по реализации политики информационной безопасности, а также весь жизненный цикл средств технической, организационной и иной

защиты информации (разработка, изготовление, испытания, эксплуатация, ремонт, хранение и утилизация) является очень важным системообразующим фактором, влияющим на эффективность функционирования всей системы защиты информации в государстве.

Поэтому создание научно обоснованной системы нормативных документов является весьма актуальной задачей, разрешение который позволит устранить существующие проблемы и недостатки правового обеспечения информационных политик.

Технические

Техническая защита информации осуществляется в несколько этапов: первый этап — определение и анализ угроз; второй этап — разработка системы защиты информации; третий этап — реализация плана защиты информации; четвертый этап — контроль за функционированием и управлением системой защиты информации [5].

Соответственно основные проблемы, возникающие с безопасностью передачи информации, можно разделить на следующие:

- перехват информации — целостность информации сохраняется, но ее конфиденциальность нарушена;
- модификация информации — исходное сообщение изменяется или полностью подменяется другим и направляется адресату;
- замена авторства информации. Данная проблема может иметь серьезные последствия. Например, кто-то может прислать письмо от чужого имени или Web-сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров.

Особую остроту технические проблемы существующих политик информационной безопасности приобретают в современных условиях, когда средства вычислительной техники и различные информационные технологии интенсивно внедряются во все области человеческой деятельности. Поскольку проблема компьютерной безопасности является многоплановой и многогранной, то необходимо разворачивать работы по технической защите информации по многим направлениям — от разработки теоретических основ информационной безопасности компьютерных систем до разработки программных и аппаратных средств технической защиты. Особое место в этом ряду должна занять защита от атак в сети Интернет и от программных закладок [6].

Из числа основных проблем, которые необходимо решать в ближайшее время, по мнению автора, можно выделить следующие:

- совершенствование определения уровней защищенности информации;
- разработка критериев защищенности информации;
- разработка функциональных наборов аппаратно-программных средств, обеспечивающих достижение определенного (заданного) уровня защищенности информации;
- разработка методов сертификации (экспертизы) аппаратно-программных средств защиты информации;
- разработка методов сертификации (экспертизы) систем защиты информации на соответствие уровням защищенности;
- разработка специальных ЭВМ, операционных систем, обеспечивающих высокий уровень защищенности информации.

Организационные

Среди широкого спектра организационных проблем выделим, по мнению автора, одну, наиболее существенную и важную, решать которую следует только за счет привлечения широкого круга высококвалифицированных специалистов — речь идет о создании системы подготовки, повышения квалификации и переподготовки специалистов по защите информации.

Эффективность усилий, направленных на защиту интересов субъектов информационных отношений, зависит, прежде всего, от умения подготовленных специалистов выявлять и оценивать угрозы; определять состояние защищенности информации; обоснованно выбирать способы ее защиты от совокупности реальных угроз; разрабатывать и внедрять системы защиты на основе требований действующего законодательства.

Аргументом целесообразности и первоочередности таких действий выступают неопровержимые факты роста в угрожающих масштабах компьютерной преступности и кибертерроризма. В сети Интернет на сегодняшний день представлено более 30000 сайтов, которые обучают компьютерному взлому [7].

Таким образом, подводя итоги проведенного исследования, можно сделать следующие выводы. Прогресс каждого государства в нынешних условиях неразрывно связан с развитием информационных систем и их защитой, что актуализирует необходимость в разработке эффективной, адаптивной и гибкой политики информационной безопасности. Однако данный процесс связан с комплексом различных проблем, среди которых можно выделить теоретические и практические. В процессе исследования автором подробно рассмотрены проблемы указанных двух групп. Результаты ана-

лиза позволяют утверждать, что в целом все названные и многие другие проблемы могут быть решены в результате создания стабильно функционирующих систем защиты информации на разных уровнях. Развитие и становление таких систем может быть реализовано только путем объединения усилий различных министерств, ведомств, организаций, учреждений, предприятий, а также усилий ученых, инженеров и практиков на пути разработки и реализации политик информационной безопасности.

ЛИТЕРАТУРА

1. Бржезинская А. Д. Создание политики информационной безопасности и ее влияние на процесс управления безопасностью // Молодежный научный форум: общественные и экономические науки. — 2016. — № 11. — С. 231–235.
2. Амиантов А.А., Волобуев К. В. Современные проблемы информационной политики в контексте национальной безопасности // Вопросы политологии. — 2016. — № 2(22). — С. 68–74.
3. Юдина Н.Ю., Лапшина М. Л. Защита информации в информационных системах // Моделирование систем и процессов. — 2016. — № 4. — С. 89–92.
4. Соколов Д. В. Реализация политики информационной безопасности в сфере законотворчества // Вопросы национальных и федеративных отношений. — 2016. — № 3(34). — С. 39–52.
5. Кукушкин С.С., Мистров Л. Е. Постановка задачи защиты информации в организационно технических системах по техническим каналам утечки // Двойные технологии. — 2017. — № 1(78). — С. 59–63.
6. Сусло С. В. Защита информации от утечки по техническим каналам // Теория и практика современной науки. — 2017. — № 5(23). — С. 786–788.
7. Титов М.Ю., Трубиенко О. В. Анализ основных подходов в создании надежной системы передачи информации // Промышленные АСУ и контроллеры. — 2017. — № 5. — С. 62–67.

Журнал «Современная наука: актуальные проблемы теории и практики»

Астраханский государственный университет