https://ru.wikipedia.org/wiki/PCMCIA – Дата доступа: 21.03.2016.

4 Википедия – свободная энциклопедия [Электронный ресурс] / Биометрические системы аутентификации – Режим доступа: https://ru.wikipedia.org/wiki/Биометрические_системы_аутентификации – Дата доступа: 22.03.2016.

УДК 003.26+347.78

Магистрант Г.А. Язкулыев
Науч. рук. проф. д-р техн. наук П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ СИТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Информация стала одним из главных факторов исторического прогресса. Она имеет ключевое значение для успешного функционирования всех общественных и государственных институтов, адекватного поведения каждого отдельного человека. Без интенсивного обмена информацией, постоянной информационной связи с окружающим миром в принципе невозможна нормальная жизнедеятельность людей.

Диалектика развития, в том числе – в области информационных технологий (ИТ), характеризуется обострением противоречий, появлением проблем. К числу важнейших в области ИТ следует отнести проблему безопасности, которая напрямую касается обеспечения безопасности систем жизнеобеспечения людей, управления транспортом, производственными процессами, коммуникациями, вооруженными силами и других систем специального назначения (ССН). Большой класс таких систем предназначен для решения задач государственного управления, управления войсками и оружием, экологически опасными и экономически важными производствами и т.п. Они часто функционируют в условиях деструктивных воздействий, целью которых является разрушение информационных ресурсов, нарушение штатных режимов функционирования и, как следствие, срыв выполнения возложенных на такие системы функций. Это определяет необходимость организации защиты ИС СН от таких воздействий [1].

Политика безопасности при этом трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. Политика безопасности описывает цели и задачи информационной безопасности (ИБ) на понятном пользователю языке и определяет направления работы подразделений ИБ. Политика безопасности зависит от:

- конкретных технологий обработки информации;

- используемых технических и программных средств;
- вида деятельности организации.

Если достаточно широко определить понятие «безопасность» по отношению к информационным технологиям, то можно сказать, что безопасность систем, занимающихся обработкой данных – это степень защищенности и способности противостоять внешним угрозам. Это процесс непрерывных, динамических, требующих постоянных усилий [2].

На практике политика безопасности трактуется несколько шире – как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. Результатом политики является высокоуровневый документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Данный документ представляет методологическую основу практических мер (процедур) по реализации обеспечение информационной безопасности и содержит следующие группы сведений:

1. Основные положения информационной безопасности,
2. Область применения,
3. Цели и задачи обеспечения информационной безопасности,
4. Распределение ролей и ответственности,
5. Общие обязанности.

Основные положения определяют важность обеспечения информационной безопасности, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

Областью применения политики безопасности являются основные активы и подсистемы автоматизированной системы, подлежащие защите. Типовыми активами являются программно-аппаратное и информационное обеспечение автоматизированной системы, персонал, в отдельных случаях – информационная инфраструктура предприятия.

Цели, задачи, критерии обеспечение информационной безопасности вытекают из функционального назначения предприятия. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности (оперативной готовности) подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т. д. Здесь указываются законы и правила организации, которые следует учитывать при проведении работ по обеспечения информационной безопасности.

Политика безопасности затрагивает всех пользователей компьютеров в организации. Поэтому важно решить так называемые организационно-правовые вопросы наделения всех категорий пользователей соответствующими правами, привилегиями и обязанностями.

Важным элементом политики является распределение ответственности. Политика не может предусмотреть всего, однако, она должна для каждого вида проблем найти ответственного [2].

На практике политика безопасности в ССН рассматриваются на более высоком уровне, в котором все аспекты должны быть тщательно разработаны.

С развитием систем специального назначение и возросшей ролью ИТ во многих странах проблема безопасности информационных ресурсов, в том числе – и разработка политики безопасности ССН – отнесена к числу первоочередных в контексте обеспечения национальной безопасности.

Понятие «информационная безопасность» на постсоветском пространстве появилось еще в мае 1992 года, когда в Ташкенте главами государств Азербайджана, Беларуси, Грузии, Казахстана, Кыргызстана, Молдовы, Таджикистана, Туркменистана, Узбекистана, Армении, Украины и России было подписано «Соглашение об обеспечении безопасности шифровальных средств» [3]. На основе этого документа создан и работает Координационный совет по обеспечению безопасности шифровальных средств и их эксплуатации в системах правительственной и закрытой ведомственной связи участников Содружества.

Постановление Межпарламентского Комитета Республики Беларусь, Республики Казахстан, Кыргызской Республики, Российской Федерации и Республики Таджикистан от 15 октября 1999 г. No 9-9 «О модельном законе «О безопасности»» определяет информационную безопасность как состояние защищенности государственных информационных ресурсов, а также прав личности и интересов общества в информационной сфере [4].

В процессе разработки политики безопасности важным элементом является нормативно правовые основы. В РБ разработан Закон № 455-З от 10.11.2008 г. «Об информации, информатизации и защите информации». В Туркменистане работы в указанной области осуществляются с учетом того, что все информационные ресурсы принадлежат государственным организациям. С развитие Интернета и информационных систем страны в Туркменистане изданы Законы в сфере средств массовой информации и Закон «О правовом регулировании развития сети интернет и оказания интернет-услуг в туркменистане» (декабрь 2014 г.). Целями и задачами этого Закона являются обеспе-

чение свободного доступа пользователей к интернету на территории Туркменистана, определение правового режима информации, размещаемой в интернете или передаваемой через интернет, предотвращение общественно опасных деяний, совершаемых в интернете, а также создание условий для эффективного выявления и наказания лиц, совершающих такие правонарушения и т.д.

Важность проблемы информационной безопасности сейчас, к сожалению, очевидна далеко не для всех. Однако даже небольшого размышления достаточно, чтобы понять ее проблемы и сложность, проистекающие как из сложности и разнородности современных информационных систем, так и из необходимости комплексного подхода к безопасности с привлечением законодательных, административных и программно-технических мер.

Систематизируя сравнительный анализ законодательств и концепций стран постсоветского пространства, можно выделить основные виды угроз информационной безопасности в странах Белоруссии и Туркменистана:

1. угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению страны;
2. угрозы информационному обеспечению государственной политики страны;
3. угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
4. угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории данной страны.

Угрозами информационному обеспечению государственной политики могут являться:

- монополизация информационного рынка страны, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию местной и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики страны вследствие дефицита

квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

ЛИТЕРАТУРА

1. Казарин, О.В. Методы и средства проактивной защиты программного обеспечения информационных систем специального назначения: диссертация: автореф. дисс. д.т.н., спец. 05.13.19, 05.25.05/ О.В. Казарин. – М.:Ин-т проблем информац. безопасности МГУ, 2012.

2. Урбанович, П.П. Защита информации и надежность информационных систем/ П.П. Урбанович, Д.В. Шиман: уч.-мет. пособие. – Минск: БГТУ, 2013. – 90 с.

3. Караев, С. Сравнительный анализ угроз информационной безопасности в странах постсоветского пространства/ С. Караев// [Электронный ресурс]: http://www.nplg.gov.ge/gsdl/cgi-bin/library.exe?e- , Дата доступа: 30.04.2016.

4. О модельном законе «О безопасности»: Постановление Межпарламентского Комитета Республики Беларусь, Республики Казахстан, Кыргызской Республики, Российской Федерации и Республики Таджикистан, 15 октября 1999 г., No 9-9 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2014.

УДК 627.8

Студ. Е.Л. Демянчук
Науч. рук. доц. Г. И. Касперов
(кафедра инженерной графики, БГТУ)

ХИМИЧЕСКОЕ ЗАГРЯЗНЕНИЕ ВОДНЫХ ОБЪЕКТОВ – ОПАСНОСТЬ ДЛЯ ОКРУЖАЮЩЕЙ СРЕДЫ

Вопросам охраны окружающей среды и решению экологической проблемы природопользования в Республике Беларусь уделяется огромное значение. Анализ литературных, научных и других источников показал, что на территории Беларуси ежегодно регистрируется до 10 аварийных ситуаций сопровождающихся химическим загрязнением водных объектов. При этом установлено, что масштабы, в особенности при авариях вблизи водных объектов, имеют большие площади распространения. Опубликованные Минприроды Республики Беларусь данные свидетельствуют о том, что поверхностные воды страны испытывают значительную химическую нагрузку. Наибольшее количество недостаточно очищенных сточных вод, содержащих различные химические компоненты и соединения, поступает в реки бассейна Днепра. Среди рек наибольшую нагрузку, связанную со сточными водами, испытывают: р. Свислочь ниже Минска, р. Неман