никновения сигналов ЧР дополнительной емкости в цепь измерительного резистора [4].

Выводы:

1 Реализована резонансная испытательная схема для испытания коротких образцов высоковольтных кабелей путем введения в состав схемы дополнительной нагрузочной емкости, подключаемой параллельно испытываемому отрезку кабеля.

2 Приведены расчет и конструкция дополнительной емкости на основе комбинированного бумажно-пленочного диэлектрика, пропитанного нефтяным маслом. Данная конструкция позволяет существенно расширить возможности испытательной схемы и имеет в 5-6 раз меньшую стоимость по сравнению с известными аналогичными конструкциями.

3 Проведен анализ результатов измерения уровня частичных разрядов на дополнительной нагрузочной емкости. Показана необходимость проведения дальнейших исследований, связанных с решением задачи по достижению уровня ИЧР не более 2 пК во всем диапазоне испытательных напряжений $U = 0 \div 160$ кВ. Обозначены возможные пути решения данной задачи.

Список литературы: 1. *Привезенцев В.А., Гроднев И.И., Холодный С.Д., Рязанов И.Б.* Основы кабельной техники / Учеб. пособ. для вузов. Под. ред. *В.А.Привезенцева*. – М.: Энергия. 1975. – 472 с. **2**. Каталог фирмы Hipotronics – 2002. – 10 с. **3**. *Кравченко Ю.В., Набока Б.Г., Рудаков В.В.* и др. Резонансная установка для испытания коротких отрезков высоковольтных кабелей // Електротехніка і електромеханіка. – 2008. – № 4. – С. 75-80. **4**. *Рудаков В.В., Набока Б.Г., Кравченко Ю.В.* и др. Повышение добротности колебательного контура резонансной установки для высоковольтных испытаний кабелей // Метрологія та прилади. – 2008. – № 2. – С. 33-37.

Поступила в редколлегию 02.09.2008.

УДК 65.012:34(477).

А.А.СЕРКОВ, докт.техн.наук, НТУ «ХПИ», Харьков;
В.Я.ПЕВНЕВ, канд.техн.наук, ХНУВС, Харьков

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: КОНЦЕПЦИЯ И СРЕДСТВА ОБЕСПЕЧЕНИЯ

Розглянуто існуючі визначення інформаційної безпеки, виявлені недоліки цих визначень. Запропоновано визначення інформаційної безпеки, які базуються на системному підході. Розглянуто функції інформаційної безпеки з точки зору властивості інформації та засобів її забезпечення

The existing determinations of information security are considered; the defects of these determinations are determined. The determination of information security, which based on system approaches are proposed. They functions of information security with standpoint of characteristics of information and facilities of there provisions are considered.

Постановка проблемы. Согласно Конституции Украины [1] обеспечение информационной безопасности (ИБ) относится к наиболее важным функциям государства. Это положение показывает место ИБ в системе безопасности всего государства. Вместе с тем в существующих законах нет понятия ИБ. Более того, оно отсутствует и в универсальной десятичной классификации [2].

Анализ литературы. В то же время существует большое количество определений, которые отражают по или иное представление ИБ. Так в работе [3] представлено следующее определение ИБ: «інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процесі в державі, що забезпечують гарантовані Конституцію умови існування і розвитку людини, всього суспільства і держави». Данное толкование ставит знак равенства между ИБ и безопасностью государства, сужая этим само понятие ИБ. В настоящее время нет закона, который бы определял ИБ и, соответственно, нет правил по которым происходит информационный процесс с точки зрения ИБ. В работе [4] подчеркивается, что «інформаційна безпека – це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від внутрішніх і зовнішніх інформаційних загроз». Это определение созвучно с понятием ИБ, которое положено в основу Доктрины информационной безопасности и законодательства в сфере обеспечения информационной безопасности Российской Федерации: «ИБ – это состояние защищенности жизненно-важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз»[5]. Данное определение также не отражает сущности ИБ, сужая его только до общественных взаимоотношений. Во многих работах и выступлениях происходит подмена понятия ИБ на безопасную информацию или безопасность информации. Это видно на примере материалов круглого стола «Информационная безопасность Украины: сущность и проблемы», проведенного в июне 1998 г. [6]. По мнению авторов, такой подход неправомерен, так как уводит от сущности ИБ. Определение ИБ не должно зависеть от того, о каком предмете идет речь. ИБ одна, и, давая определение, нужно исходить из этого.

Цель статьи – обосновать понятие информационной безопасности и ее составляющих.

Определение ИБ. Исторически понятие ИБ появилось механическим переводом английского термина information security. Равнозначным его пере-

водом является и защита информации.

Когда говорят об ИБ, то речь должна идти о какой-либо системе, будь то государство, корпорация, телекоммуникационная сеть или что-то другое. Согласно [7], под системой понимается объединение некоторого разнообразия в единое и четко расчлененное целое, элементы которого по отношению к целому и другим частям занимают соответствующие им места. Каждая система обладает рядом свойств и может находиться в том или ином состоянии. По аналогии с надежностью [8], говоря об ИБ надо рассматривать не состояния, а свойства системы. Таким образом, можно сказать, что ИБ – это свойство системы. Понятие ИБ всегда должно быть логически привязано к информации, средствам ее обработки, хранения, доставки, воздействия на объект. В жизненном цикле информация может быть подвергнута различного вида воздействиям, которые направлены на нарушения конфиденциальности, целостности и доступа к информации [9].

Исходя из вышеизложенного, предлагается следующее определение ИБ: ***информационная безопасность – свойство системы противостоять несанкционированному снятию и модификации информации.***

Под несанкционированным снятием понимается получение информации, к которой у абонента нет доступа, т.е. нарушение правил доступа. А под несанкционированной модификацией понимается изменение информации, которое приводит к нарушению ее целостности. Следует отметить, что целостность, в общем случае, это не только полученная информация в исходном виде, но и ее полнота.

Исходя из представленного определения, можно рассмотреть составляющие ИБ. В первую очередь необходимо говорить о конфиденциальности информации. Согласно [10], «конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов». Основываясь на положение Закона, ставиться задача на ограничение доступа к тому или иному виду информации. При решении этой задачи можно говорить о двух направлениях: первое – работа с законопослушными пользователями информации, которые выполняют все инструкции по организации допуска, и второе – когда речь идет о преднамеренном снятии закрытой информации. В этом случае необходимо проводить ряд организационных и технических мероприятий по защите информации.

Таким образом, можно определить первую функцию ИБ – это организация работ по ограничению доступа к информации.

Особое значение при этом придается целостности информации. Большинство исследователей не привязывает целостность к конкретной системе. Рассмотрим это на примере функционирования двух систем – государства и телевидения. В прямом эфире выступает один из политиков и излагает какие-либо сведения, говоря при этом не всю правду. С точки зрения государства

целостность информации нарушена. С точки зрения телевизионной системы информация доведена полностью, и она является целостной, так как не была искажена в процессе передачи. При этом ошибочным является и понятие о том, что система должна обеспечить целостность информации. Логично было бы говорить о проверке на целостность. Обеспечение целостности требует огромного числа правовых, организационных и технических мероприятий, позволяющих предотвратить нарушение целостности информации, а реализовать это требование на современном этапе развития практически не возможно.

В тоже время, проверка на целостность широко используется в различных системах. Для этого используют цифровую подпись. Данный инструментарий достаточно полно прописан в законодательстве Украины [11,12]. При этом следует отметить, что при организации систем связи используется помехоустойчивое кодирование, которое позволяет восстанавливать искаженную информацию. Таким образом, следует выделить и сформулировать вторую функцию ИБ – контроля и, по возможности, обеспечения целостности информации.

Говоря о целостности сообщения, интуитивно возникает вопрос об авторстве полученной информации. Решением этого вопроса занимаются специалисты во многих отраслях, но наиболее критичным он становится в банковской сфере. Определение авторства (аутентификация) происходит с помощью цифровой подписи, а точнее, ключа к этой подписи. Сложнее процесс аутентификации происходит в системах многоадресной передачи. При решении данной позиции можно было бы успешно бороться с хакерами и распространителями вирусов в компьютерных системах. Одновременно с вопросом аутентификации возникает проблема неотрекаемости или апеллируемости. Таким образом, формулируется следующая функция ИБ – аутентификации и неотрекаемости.

Рассмотрим следующую составляющую ИБ – доступность. Она частично относится к конфиденциальности, т.е. ограничении (разграничении) доступа. Если информация не является закрытой, то она должна быть доступной для всех. Причем информация должна быть доступна в любой момент времени. В этом случае возникает проблема организации свободного доступа к официально доступной информации. Однако, достаточно часто, путем блокирования как организационными, так и техничными способами производится ограничения доступа к той или иной информации.

Средства обеспечения ИБ. Для обеспечения ИБ необходимо применять юридические и морально-этические нормы (МЭН), технические средства защиты информации (ТСЗИ).

Говоря о юридических нормах, следует отметить отсутствие в стране закона об ИБ. Такой закон мог бы позволить провести изменения в другие законы и кодексы, например, обязать руководителей предприятий занимать-

ся вопросами ИБ на стадии разработки проекта, а не после утечки информации. Возможно также внести ответственность за распространение неправдивой информации, причем чтобы это положение касалось бы не только рекламодателей, но и распространителей информации. При создании мирового информационного пространства, которым в настоящее время является Интернет, предполагалось, что все пользователи будут соблюдать неписанные правила, определяющие их поведение. В этих правилах предполагалось, что ни один из пользователей не совершит никаких действий, в результате которых будет нанесен урон другим пользователям. Как видно на примере современных пользователей, каждый из которых имеет по несколько антивирусных программ, о МЭН поведения в информационном пространстве речи не идет.

Необходимо отметить еще одну особенность использования МЭН при обеспечении ИБ различных систем, при которой вопросы соблюдения этих норм, в особенности политической элитой, выходят на первый план, а мероприятия по обеспечению ИБ предприятия МЭН необходимо учитывать при наборе сотрудников. В обеспечении ИБ наиболее важная роль принадлежит ТСЗИ. Нарушитель не остановится ни перед законом, ни перед МЭН. Единственное, что его может остановить – это ТСЗИ. Под ТСЗИ понимаются устройство и (или) программное средство, в которых функция защиты информации является основной [13]. В современном мире это большой арсенал средств противодействия любителям незаконного снятия информации.

Выводы. Представленное в работе определение ИБ отражает сущность этого термина, не привязываясь к конкретной системе. Рассмотрены функции систем ИБ и средства обеспечения этих функций.

Список литературы: 1. Конституция України. – К., 2006. – 80 с. **2.** Універсальна десяткова класифікація: У 2 кн. / Голвн.ред. *М.І.Сенченко*; UDC Consortsm, Кн. палата України. – К.: Кн. палата України, 2000. – 932 с. **3.** *Кормич Б.А.* Інформаційна безпека: організаційно-правові основи. Навч. посібник. – К.: Кондор, 2004. – 384 с. **4.** *Богуш В.М., Юдин О.К.* Інформаційна безпека держави. – К.: «МК-Прес». 2005. – 432 с. **5.** *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации / Учеб. пособие для вузов. – М.: Горячая линия - Телеком, 2004. – 280 с. **6.** Інформаційна безпека України: сутність та проблеми. Матеріали круглого столу. // www/nirr.gov.ua/ukr/publishing/panorama3_4. **7.** Философский энциклопедический словарь. – М.: ИНФРА-М, 2000. – 576 с. **8.** Новый энциклопедический словарь. – М.: Большая Российская энциклопедия, РИПОЛ Классик, 2004. – 1456 с. **9.** *Гринберг А.С., Горбачев Н.Н., Тепляков А.А.* Защита информационных ресурсов государственного управления: Учеб. пособие для вузовю – М.: ЮНИТИ-ДАНА, 2003. – 327 с. **10.** Закон України «Про інформацію» // Відомості Верховної Ради. – 1992. – № 48. **11.** Закон України «Про електронний цифровий підпис» // Відомості Верховної Ради. – 2003. – № 36. **12.** ДСТУ 4145-2002. Національний стандарт України. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. – К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003. – 31 с. **13.** ДСТУ 3396.2-97. Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення. – К.: Держстандарт України, 1997. – 20 с.

Поступила в редколлегию 16.09.2008.