Ю. М. БЕКЕТНОВА, Г. О. КРЫЛОВ, С. Л. ЛАРИОНОВА

МЕЖДУНАРОДНЫЕ ОСНОВЫ И СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВО-ЭКОНОМИЧЕСКИХ СИСТЕМ

Юлия Бекетнова

Международные основы и стандарты информационной безопасности финансово-экономических систем

«Прометей»
2018

УДК 004.056(073)
ББК 67.401.114я73

Бекетнова Ю. М.

Международные основы и стандарты информационной безопасности финансово-экономических систем / Ю. М. Бекетнова — «Прометей», 2018

ISBN 978-5-907003-27-9

Издание предназначено для студентов, обучающихся по специальности «Информационная безопасность» бакалавриата и магистратуры, а также научных работников, преподавателей, аспирантов, интересующихся проблемами теории и практики обеспечения информационной безопасности. Изложены международные основы и стандарты информационной безопасности. В формате a4.pdf сохранен издательский макет.

УДК 004.056(073)
ББК 67.401.114я73

ISBN 978-5-907003-27-9

Содержание

Юлия Михайловна Бекетнова, Григорий Олегович Крылов, Светлана Львовна Ларионова Международные основы и стандарты информационной безопасности финансово-экономических систем

Сокращения, принятые в издании

1. Нормативные правовые акты

Всеобщая декларация прав человека – Всеобщая декларация прав человека, принята Генеральной Ассамблеей ООН 10 декабря 1948 г. // Рос. газ. 1995. 5 апр.

Конвенция о защите прав человека – Конвенция о защите прав человека и основных свобод, заключена в Риме 4 ноября 1950 г. // СЗ РФ. 2001. № 2. Ст. 63.

Международный пакт о гражданских и политических правах – Международный пакт о гражданских и политических правах от 16 декабря 1966 г. // БВС РФ. 1994. № 12.

Окинавская хартия – Окинавская хартия глобального информационного общества, принята на о. Окинава 22 июля 2000 г. // Дипломатический вестник. 2000. № 8. С. 51–56

2. Официальные издания

БВС – Бюллетень Верховного Суда
ВСНД и ВС – Ведомости Съезда народных депутатов и Верховного Совета
Рос. газ. – «Российская газета»
СЗ – Собрание законодательства

3. Прочие сокращения

ГОСТ – государственный стандарт
ИБ – информационная безопасность
ИИ – информационные инфраструктуры
БС РФ – банковская система Российской Федерации
НСД – несанкционированный доступ
АБС – автоматизированная банковская система
ДБО – дистанционное банковское обслуживание
СКУД – система контроля и управления доступом
СКЗИ – средства криптографической защиты информации
АРМ – автоматизированное рабочее место
ИКТ – информационно-коммуникационные технологии
дол. – доллар (-ы)
ВТО – Всемирная торговая организация
ЕврАзЭС – Евразийское экономическое сообщество
ЕЭК – Европейская экономическая комиссия
ИСО – Международная организация по стандартизации
МЭК – Международная электротехническая комиссия
ООН – Организация Объединенных Наций
п. – пункт (-ы)
РФ – Российская Федерация
СНГ – Содружество Независимых Государств
СССР – Союз Советских Социалистических Республик
ст. – статья (-и)
США – Соединенные Штаты Америки
тыс. – тысяча (-и)
ч. – часть (-и)

Предисловие

Учебное пособие подготовлено в соответствии с государственным образовательным стандартом с учетом достижений в области обеспечения информационной безопасности, на основе анализа действующего законодательства и международной практики.

В пособии исследованы понятие и сущность международного информационного права, законодательство и лучшие практики в данной области, включая область защиты конфиденциальной информации, управления информационной безопасностью, изучены конституционные гарантии прав граждан на информацию и механизм их реализации, понятие и виды защищаемой информации по законодательству РФ, рассмотрены вопросы правового регулирования взаимоотношений администрации и персонала в области защиты информации, лицензирования и сертификации данной отрасли, защиты информации с использованием технических средств и защиты интеллектуальной собственности, проанализированы виды правонарушений в сфере компьютерной информации.

Учебное пособие может использоваться студентами высших учебных заведений, обучающихся по направлению «Информационная безопасность».

Авторы выражают признательность рецензентам – доктору военных наук, кандидату технических наук, профессору, заслуженному работнику связи РФ, профессору кафедры безопасности радиосвязи Московского технического университета связи и информатики Александру Николаевичу Кубанкову и кандидату технических наук, заместителю заведующего кафедрой информационной безопасности Финансового университета при Правительстве РФ Александру Жакферовичу Низамову за ценные замечания, помощь и поддержку при подготовке учебного пособия.

Глава 1. Основы международного информационного права

1.1. Защита прав человека

Среди методов обеспечения информационных прав и свобод основными являются методы нормативно-правового регулирования общественных отношений в информационной сфере, а в силу глобализации информационного общества большое значение имеют информационные институты международного права. Важным институтом международного права в информационной сфере являются общие нормы, касающиеся информационных прав и свобод человека и защиты информационной инфраструктуры.

Главным международным источником прав человека и его основных свобод является Всеобщая декларация прав человека.

Так, ст. 2 Декларации определяет норму принадлежности каждому человеку всех прав и свобод независимо от расы, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения.

Согласно ст. 11 Декларации каждый человек, обвиняемый в совершении преступления, имеет право считаться невиновным до тех пор, пока его виновность не будет установлена законным порядком путем гласного судебного разбирательства, при котором ему обеспечиваются все возможности для защиты.

Никто не может подвергаться вмешательству в личную и семейную жизнь, произвольным посягательствам на неприкосновенность жилища, тайну корреспонденции или на честь и репутацию (ст. 12).

Статья 19 Декларации наделяет каждого человека правом на свободу убеждений и свободное их отражение; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами независимо от государственных границ.

Наконец, согласно ч. 1 ст. 27 каждый человек имеет право свободно участвовать в культурной жизни общества, наслаждаться искусством, участвовать в научном прогрессе и пользоваться его благами.

Часть 2 этой же статьи наделяет каждого человека правом на защиту его моральных и материальных интересов, являющихся результатом научных, литературных или художественных трудов, автором которых он является.

Положения Всеобщей декларации прав человека, закрепляющие информационные права и свободы, развивает Конвенция о защите прав человека.

Так, в ч. 1 ст. 10 Конвенции каждому человеку предоставлено право на свободу выражать свое мнение. Это право включает свободу придерживаться своего мнения и свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны государственных органов и независимо от государственных границ.

Однако в ч. 2 этой же статьи констатируется, что государствам можно осуществлять лицензирование радиовещательных, телевизионных или кинематографических предприятий. Указано также, что осуществление этих свобод может ограничиваться в интересах государственной безопасности, территориальной целостности или общественного спокойствия, в целях предотвращения беспорядков, для охраны здоровья и нравственности, защиты репутации и прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия.

1.2. Пакт о гражданских и политических правах

В нашей стране впервые информационные права и свободы были провозглашены после ратификации Международного пакта о гражданских и политических правах. Рассмотрим основные статьи Пакта, закрепляющие эти права и свободы.

Статья 2. Каждое участвующее в настоящем Пакте государство обязуется уважать и обеспечивать всем находящимся в пределах его территории под его юрисдикцией лицам права, признаваемые в настоящем Пакте, без какого бы то ни было различия, как то: в отношении расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного положения, рождения или иного обстоятельства.

Статья 4. Во время чрезвычайного положения в государстве, при котором жизнь нации находится под угрозой и о наличии которого официально объявляется, участвующие в настоящем Пакте государства могут принимать меры в отступление от своих обязательств по настоящему Пакту только в такой степени, в какой это требуется остротой положения, при условии, что такие меры не являются несовместимыми с их другими обязательствами по международному праву и не влекут за собой дискриминации исключительно на основе расы, цвета кожи, пола, языка, религии или социального происхождения. Любое участвующее в настоящем Пакте государство, использующее право отступления, должно немедленно информировать другие государства, участвующие в настоящем Пакте, через посредство Генерального секретаря ООН о положениях, от которых оно отступило, и о причинах, побудивших к такому решению. Также должно быть сделано сообщение через того же посредника о той дате, когда оно прекращает такое отступление.

Статья 14. Все лица равны перед судами и трибуналами. Каждый имеет право при рассмотрении любого уголовного обвинения, предъявляемого ему, или при определении его прав и обязанностей в каком-либо гражданском процессе на справедливое и публичное разбирательство дела компетентным, независимым и беспристрастным судом, созданным на основании закона. Печать и публика могут не допускаться на все судебное разбирательство или часть его по соображениям морали, общественного порядка или государственной безопасности в демократическом обществе, или когда того требуют интересы частной жизни сторон, или – в той мере, в какой это, по мнению суда, строго необходимо, – при особых обстоятельствах, когда публичность нарушала бы интересы правосудия; однако любое судебное постановление по уголовному или гражданскому делу должно быть публичным, за исключением тех случаев, когда интересы несовершеннолетних требуют другого или когда дело касается матримониальных споров или опеки над детьми.

Статья 17. Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств. Осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц.

Статья 19. Каждый человек имеет право беспрепятственно придерживаться своих мнений. Каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору. Пользование предусмотренными в п. 2 настоящей статьи правами налагает особые обязанности и особую ответственность. Оно может быть, следовательно, сопряжено с некоторыми ограничениями, которые, однако,

должны быть установлены законом и являться необходимыми: а) для уважения прав и репутации других лиц; б) для охраны государственной безопасности, общественного порядка, здоровья и нравственности населения.

Статья 20. Всякая пропаганда войны должна быть запрещена законом. Всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию, должно быть запрещено законом.

Статья 40. Участвующие в настоящем Пакте государства обязуются представлять доклады о принятых ими мерах по претворению в жизнь прав, признаваемых в настоящем Пакте, и о прогрессе, достигнутом в пользовании этих прав.

1.3. Охрана информационной инфраструктуры

Важнейшим объектом международного права являются общественные отношения, касающиеся информационной инфраструктуры. Следует отметить, что формирование международно-правового режима информационной инфраструктуры значительно отстает от темпов развития информационного общества. Тем не менее, отдельные виды отношений в этой области регулируются международными нормами. Источниками этих норм, в частности, являются:

– международное гуманитарное право, регулирующее правила ведения вооруженных конфликтов;

– Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела (подписан в Вашингтоне, Лондоне, Москве 27 января 1967 г.)[1];

– документы Международного союза электросвязи;

– международные стандарты в области магнитных и интеллектуальных карт и др.

Приведем некоторые нормы, обеспечивающие безопасность информационной инфраструктуры.

Так, установка приемо-передающих станций не должна мешать коммуникациям других государств. Международными соглашениями упорядочен, например, порядок занятия точек стояния космических аппаратов на геостационарной орбите с целью исключения взаимных влияний.

Воспрещается передавать ложные сигналы бедствия, поскольку они накладывают обязательства на всех, кто способен оказать помощь терпящим бедствие.

В интересах защиты информационной инфраструктуры нейтральных держав участникам вооруженного конфликта запрещено использовать средства связи нейтральных стран. Вместе с тем любые средства передачи сообщений противника разрешается захватывать. В то же время запрещено уничтожать (повреждать) подводные кабели между занятой территорией и нейтральными государством.

В последнее время в связи с ростом электронных услуг в различных сферах жизни общества введены стандарты на размеры, шрифт и архитектуру безопасности магнитных и интеллектуальных карт.

Важнейшей отраслью международного права, регулирующей правила ведения вооруженных конфликтов и содержащей нормы регулирования отношений в информационной сфере, является международное гуманитарное право.

[1] См.: ВВС СССР. 1967. № 44. Ст. 588.

1.4. Нормы международного гуманитарного права в информационной сфере

Принципы, источники и объекты международного гуманитарного права. Основными принципами международного гуманитарного права являются:

– гуманизация вооруженных конфликтов;

– ограничение воюющих в выборе методов и средств ведения войны;

– международно-правовая защита жертв войны;

– охрана гражданских объектов и культурных ценностей;

– защита интересов нейтральных государств.

Наиболее важными источниками международного гуманитарного права считаются следующие документы:

– IV Гаагская конвенция о законах и обычаях сухопутной войны, заключена в Гааге 18 октября 1907 г.[2];

– Женевская конвенция о защите гражданского населения во время войны, заключена в Женеве 12 августа 1949 г.[3];

– Женевская конвенция об обращении с военнопленными, заключена в Женеве 12 августа 1949 г.[4];

– Женевская конвенция об улучшении участи раненых, больных и лиц, потерпевших кораблекрушение, из состава вооруженных сил на море, заключена в Женеве 12 августа 1949 г.[5];

– дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов (Протокол I), подписан в Женеве 8 июня 1977 г.[6];

– дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв вооруженных конфликтов немеждународного характера (Протокол II), подписан в Женеве 8 августа 1977 г.[7];

– Конвенция о защите культурных ценностей в случае вооруженного конфликта, заключена в Гааге 14 мая 1954 г.[8];

– Конвенция о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие, заключена в Женеве 10 октября 1980 г.[9]

Основными объектами защиты гуманитарного права в информационной сфере являются:

– гражданское население;

– комбатанты и некомбатанты;

– лица, находящиеся во власти участвующей в конфликте стороны;

---

[2] См.: Действующее международное право в 3 т. Т. 2. М., 1997. С. 575–587.

[3] См.: Международная защита прав и свобод человека: сб. док. М., 1990. С. 512–569.

[4] Там же. С. 454–512.

[5] См.: Там же. С. 436–453.

[6] См.: Там же. С. 570–635.

[7] См.: Там же. С. 647–658.

[8] См.: ВВС СССР. 1957. № 3. Ст. 54.

[9] См.: Там же. 1984. № 3. Ст. 50.

– жертвы войны (погибшие и раненые);
– военнопленные;
– культурные ценности и места отправления культа;
– учреждения, служащие целям науки и искусства, а также исторические памятники.

Основные нормы гуманитарного права в информационной сфере. Защита гражданского населения в информационной сфере регламентирована следующими нормами:
– введен запрет на принуждение граждан давать какие-либо сведения при любых обстоятельствах;
– запрещено также принуждать граждан присягать на верность новой власти;
– ответственность за деяния отдельных лиц воспрещается возлагать на все население или группу лиц;
– участники конфликта обязаны уважать семейную честь и права гражданского населения, убеждения каждого гражданина;
– если производится изъятие в виде контрибуции какого-либо имущества, то обязательным является удостоверение контрибуции в письменной форме с надлежащим оформлением;
– запрещено обязывать гражданских лиц участвовать в войне против своего отечества.
В отношении лиц, находящихся во власти конфликтующей стороны, предусмотрены нормы, обеспечивающие их защиту в информационной сфере:
– участники конфликта обязаны любыми путями оказывать помощь в воссоединении семей;
– кроме того, на них налагается обязанность документально удостоверять факт и адрес эвакуации детей;
– наложен запрет на надругательство над человеческим достоинством;
– журналисты, выполняющие свои функции в войсках, защищаются как гражданские лица;
– запрещено насилие над психическим состоянием лиц;
– в случае ареста лица, оно должно быть немедленно проинформировано о причинах ареста на понятном ему языке.

Международное гуманитарное право предусматривает следующие основные нормы защиты жертв войны в информационной сфере:
– участники конфликта обязаны оказывать уважение жертвам войны;
– конфликтующие стороны извещают друг друга о расположении своих медицинских стационаров;
– медицинскому и духовному персоналу, оказывающим помощь жертвам войны, предоставляются отличительные знаки, сигналы, удостоверения. Этот персонал защищается как гражданские лица.

Над жертвами войны запрещены медицинские и научные эксперименты.
Медицинскому персоналу запрещено предоставлять какую-либо информацию о больных.
Особой защитой международного гуманитарного права в информационной сфере пользуются военнопленные:
– военнопленные обязаны сообщать только свои фамилию, имя и отчество, дату рождения и личный номер;
– участники конфликта обязаны без промедления снабжать военнопленных удостоверением личности;
– деньги у военнопленных отбираются только под расписку;

– при эвакуации составляются списки военнопленных;
– военнопленным предоставляется полная свобода отправления религиозных обрядов;
– кроме того, поощряется интеллектуальная активность военнопленных.

Важным объектом защиты международного гуманитарного права являются культурные ценности и учреждения науки и культуры:

– участникам конфликта запрещается совершать враждебные акты против того, что составляет духовное наследие народов;

– запрещено также использование того, что составляет духовное наследие народов, для поддержки военных усилий;

– стороны конфликта обязаны предотвращать вывоз культурных ценностей с оккупированных территорий.

Помимо норм гуманитарного права, регулирующих отношения в информационной сфере в военное время, в современных условиях очень важно международное сотрудничество при противодействии компьютерным правонарушениям. Это связано с характерной особенностью компьютерных правонарушений – их трансграничным характером.

Глава 2. Международные проблемы противодействия правонарушениям в сфере компьютерной информации

2.1. Классификация и признаки компьютерных правонарушений

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных правонарушений. Ниже приведены названия способов совершения подобных правонарушений, соответствующих кодификатору Генерального секретариата Интерпола. В 1991 г. данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен национальным центральным бюро Интерпола более чем 100 стран.

Все коды, характеризующие компьютерные правонарушения, имеют идентификатор, начинающийся с буквы *Q*. Для характеристики правонарушений могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

1. *QA* – несанкционированный доступ и перехват:
– *QAH* – компьютерный абордаж;
– *QAI* – перехват;
– *QAT* – кража времени;
– *QAZ* – прочие виды несанкционированного доступа и перехвата.
2. *QD* – изменение компьютерных данных:
– *QUL* – логическая бомба;
– *QDT* – троянский конь;
– *QDV* – компьютерный вирус;
– *QDW* – компьютерный червь;
– *QDZ* – прочие виды изменения данных.
3. *QF* – компьютерное мошенничество:
– *QFC* – мошенничество с банкоматами;
– *QFF* – компьютерная подделка;
– *QFG* – мошенничество с игровыми автоматами;
– *QFM* – манипуляции с программами ввода-вывода;
– *QFP* – мошенничества с платежными средствами;
– *QFT* – телефонное мошенничество;
– *QFZ* – прочие компьютерные мошенничества.
4. *QR* – незаконное копирование:
– *QRG* – компьютерные игры;
– *QRS* – прочее программное обеспечение;
– *QRT* – топография полупроводниковых изделий;
– *RZ* – прочее незаконное копирование.
5. *QS* – компьютерный саботаж:
– *QSH* – с аппаратным обеспечением;
– *QSS* – с программным обеспечением;
– *QSZ* – прочие виды саботажа.
6. *QZ* – прочие компьютерные преступления:
– *QZB* – с использованием компьютерных досок объявлений;
– *QZE* – хищение информации, составляющей коммерческую тайну;

– *QZS* – передача информации конфиденциального характера;

– *QZZ* – прочие компьютерные правонарушения.

Кратко охарактеризуем некоторые виды компьютерных правонарушений согласно приведенному кодификатору.

Несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных правонарушений:

1. *QAH* – «компьютерный абордаж» (от англ. – *hacking*): доступ в компьютер или сеть без права на то. Этот вид компьютерных правонарушений обычно используется хакерами для проникновения в чужие информационные сети.

2. *QAI* – перехват *(interception)*: перехват при помощи технических средств без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений относится и электромагнитный перехват *(electromagnetic pickup)*. Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т. д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата.

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая специфическая терминология:

– «жучок» *(bugging)* – установка микрофона в компьютере с целью перехвата разговоров;

– «откачивание данных» *(data leakage)* – сбор информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;

– «уборка мусора» *(scavenging)* – поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности – физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т. д. Электронный вариант требует исследования данных, оставленных в памяти машины;

– метод «следования за дураком» *(pigbacking)* – несанкционированное проникновение как в пространственные, так и в электронные закрытые зоны. Суть метода состоит в несанкционированном проникновении в закрытые зоны следом за законным пользователем или вместе с ним;

– метод «за хвост» *(between the lines entry)*, используя который, можно подключиться к линии связи законного пользователя и, дождавшись, когда последний закончит активный режим, продолжать осуществлять доступ к системе от его имени;

– метод «неспешного выбора» *(browsing)*. В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите системы. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;

– метод «поиск бреши» *(trapdoor entry)*, при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;

– метод «люк» *(trapdoor)*, являющийся развитием предыдущего. В найденной «бреши» программа «разрывается» и в нее вставляется определенное число команд. По мере необходимости «люк» открывается, а встроенные команды автоматически осуществляют свою задачу;

– метод «маскарад» *(masquerading)*. В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;

– метод «мистификация» *(spoofi ng)*, который используется при случайном подключении чужой системы.

Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя.

3. *QAT* – кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.

Изменение компьютерных данных (QD) включает в себя следующие виды правонарушений:

1. *QDL / QDT* – логическая бомба *(logic bomb)*, троянский конь *(trojan horse)*: изменение компьютерных данных без права на то путем внедрения логической бомбы или троянского коня. Логическая бомба тайно встраивается в программу набора команд, который должен сработать лишь однажды, но при определенных условиях. Троянский конь – способ, заключающийся в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

2. *QDV* – вирус *(virus)*: изменение компьютерных данных или программ без права на то путем внедрения или распространения компьютерного вируса. Компьютерный вирус – это специально написанная программа, которая может «приписать» себя к другим программам (т. е. заражать их), размножаться и порождать новые вирусы для выполнения различных нежелательных действий в компьютере. Процесс заражения компьютера программой-вирусом и его последующее лечение имеют ряд черт, свойственных медицинской практике. По крайней мере, эта терминология весьма близка к медицинской:

– резервирование – копирование FAT (от англ. *file allocation table* – «таблица размещения файлов»), ежедневное ведение архивов измененных файлов – самый важный и основной метод защиты от вирусов. Остальные методы не могут заменить ежедневного архивирования, хотя и повышают общий уровень защиты;

– профилактика – раздельное хранение вновь полученных и уже эксплуатируемых программ, разбиение дисков на «непотопляемые отсеки» – зоны с установленным режимом «только для чтения», хранение неиспользуемых программ в архивах, использование специальной «инкубационной» зоны для записи новых программ с дискет, систематическая проверка загрузочного сектора используемых дискет и др.;

– анализ – ревизия вновь полученных программ специальными средствами и их запуск в контролируемой среде, систематическое использование контрольных сумм при хранении и передаче программ. Каждая новая программа, полученная без контрольных сумм, должна тщательно проверяться компетентными специалистами по меньшей мере на известные виды компьютерных вирусов, и в течение определенного времени за ней должно быть организовано наблюдение;

Конец ознакомительного фрагмента.