Раздел 4. ЦИФРОВАЯ ЭКОНОМИКА И НОВЫЕ РИСКИ ДЛЯ ГОСУДАРСТВА

4.1 Аппаратно-программные комплексы защиты информации

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается уязвимость защиты информации. При этом основными **факторами, способствующими повышению этой уязвимости**, являются: резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ (Электронно-вычислительной машины) и других средств автоматизации; сосредоточение в единых базах данных информации различного назначения и различных принадлежностей; резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней данных; усложнение режимов функционирования технических средств вычислительных систем: широкое внедрение многопрограммного режима, а также режимов разделения времени и реального времени; автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях.

В этих условиях возникает **уязвимость двух видов**: с одной стороны, возможность уничтожения или искажения информации (т.е. нарушение ее физической целостности), а с другой – возможность несанкционированного использования информации (т.е. опасность утечки информации ограниченного пользования).

Основными **потенциально возможными каналами утечки информации** являются: прямое хищение носителей и документов; запоминание или копирование информации; несанкционированное подключение к аппаратуре и линиям связи или несанкционированное использование законной (т.е. зарегистрированной) аппаратуры системы (чаще всего терминалов пользователей).

Для защиты от всех этих угроз разрабатываются и применяются специальные **средства защиты информации**. Средства защиты информации – это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Средства обеспечения защиты информации разделяются на следующие группы (виды): аппаратные, программные, смешанные, организационные.

Аппаратные (технические) средства – это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки.

Первую часть задачи решают замки, решетки на окнах, сторожа, защитная сигнализация и др. Вторую – генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, перекрывающих потенциальные каналы утечки информации или позволяющие их обнаружить.

Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Их слабые стороны: недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств: универсальность, гибкость, надежность, простота установки, способность к модификации и развитию.

Их недостатки: ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций,

высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия).

Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Их недостатки: высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

Рассмотрим теперь более подробно аппаратные средства защиты информации.

К **аппаратным средствам защиты информации** относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

- специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;

- устройства измерения индивидуальных характеристик человека (голоса, отпечатков пальцев) с целью его идентификации;

- схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных;

- устройства для шифрования информации (криптографические методы).

При этом для защиты периметра информационной системы создаются: системы охранной и пожарной сигнализации; системы цифрового видео наблюдения; системы контроля и управления доступом.

Защита информации от ее утечки техническими каналами связи обеспечивается следующими **средствами и мероприятиями**:

- использование экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;

- установка на линиях связи высокочастотных фильтров;

- построение экранированных помещений («капсул»);

- использование экранированного оборудования; установка активных систем зашумления; создание контролируемых зон.

Использование аппаратных средств защиты информации позволяет решать следующие **задачи**:

- проведение специальных исследований технических средств на наличие возможных каналов утечки информации;

- выявление каналов утечки информации на разных объектах и в помещениях;

- локализация каналов утечки информации;

- поиск и обнаружение средств промышленного шпионажа;

- противодействие НСД (несанкционированного доступа) к источникам конфиденциальной информации и другим действиям.

По назначению **аппаратные средства классифицируют** на средства обнаружения, средства поиска и детальных измерений, средства активного и пассивного противодействия. При этом по техническим возможностям средства защиты информации могут быть общего назначения, рассчитанные на использование непрофессионалами с целью получения общих оценок, и профессиональные комплексы, позволяющие проводить тщательный поиск, обнаружение и измерение всех характеристик средств промышленного шпионажа.

Поисковую аппаратуру можно подразделить на аппаратуру поиска средств съема информации и исследования каналов ее утечки.

Аппаратура первого типа направлена на поиск и локализацию уже внедренных средств несанкционированное доступа. Аппаратура второго типа предназначается для выявления каналов утечки информации. Определяющими для такого рода систем являются оперативность исследования и надежность полученных результатов.

Профессиональная поисковая аппаратура, как правило, очень дорогостоящая, и требует высокой квалификации работающего с ней специалиста. В связи с этим, позволить ее могут себе организации, постоянно проводящие соответствующие обследования. Конечно, это не значит, что нужно отказаться от использования средств поиска самостоятельно. Но доступные поисковые средства достаточно просты и позволяют проводить профилактические мероприятия в промежутке между серьезными поисковыми обследованиями.

Рассмотрим теперь применяемые на практике различные виды **аппаратных средств защиты информации** (АС).

Так, специализированная сеть хранения SAN (Storage Area Network) обеспечивает данным гарантированную полосу пропускания, исключает возникновение единой точки отказа системы, допускает практически неограниченное масштабирование как со стороны серверов, так и со стороны информационных ресурсов. Для реализации сетей хранения наряду с популярной технологией Fiber Channel в последнее время все чаще используются устройства iSCSI (Internet Small Computer System Interface). Дисковые хранилища отличаются высочайшей скоростью доступа к данным за счет распределения запросов чтения/записи между несколькими дисковыми накопителями. Применение избыточных компонентов и алгоритмов в RAID массивах предотвращает остановку системы из-за выхода из строя любого элемента – так повышается доступность. Доступность, один из показателей качества информации, определяет долю времени, в течение которого информация готова к использованию, и выражается в процентном виде: например, 99,999% («пять девяток») означает, что в течение года допускается простой информационной системы по любой причине не более 5 минут.

Удачным сочетанием большой емкости, высокой скорости и приемлемой стоимости в настоящее время являются решения с использованием накопителей Serial ATA и SATA.

Ленточные накопители (стримеры, автозагрузчики и библиотеки) по-прежнему считаются самым экономичным и популярным решением создания резервной копии. Они изначально созданы для хранения данных, предоставляют практически неограниченную емкость (за счет добавления картриджей), обеспечивают высокую надежность, имеют низкую стоимость хранения, позволяют организовать ротацию любой сложности и глубины, архивацию данных, эвакуацию носителей в защищенное место за пределами основного офиса.

С момента своего появления магнитные ленты прошли пять поколений развития, на практике доказали свое преимущество и по праву являются основополагающим элементом практики backup (резервного копирования).

Помимо рассмотренных технологий следует также упомянуть обеспечение **физической защиты данных** (разграничение и контроль доступа в помещения, видеонаблюдение, охранная и пожарная сигнализация), организация бесперебойного электроснабжения оборудования.

Рассмотрим теперь некоторые **примеры аппаратных средств** (АС).

АС eToken – Электронный ключ eToken – персональное средство авторизации, аутентификации и защищенного хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП). eToken выпускается в форм-факторах USB-ключа, смарт-карты или брелока. Модель eToken NG-OTP имеет встроенный генератор одноразовых паролей. Модель eToken NG-FLASH имеет встроенный модуль flash-памяти объемом до 4 ГБ. Модель eToken PASS содержит только генератор одноразовых паролей. Модель eToken PRO (Java) аппаратно реализует генерацию ключей ЭЦП и формирование ЭЦП. Дополнительно eToken могут иметь встроенные бесконтактные радио-метки (RFID-метки), что позволяет использовать eToken также и для доступа в помещения.

Модели eToken следует использовать для аутентификации пользователей и хранения ключевой информации в автоматизированных системах, обрабатывающих конфиденциальную

информацию, до класса защищенности 1Г включительно. Они являются рекомендуемыми носителями ключевой информации для сертифицированных СКЗИ (КриптоПро CSP, Крипто-КОМ, Домен-К, Верба-OW и др.)

АС Комбинированный USB-ключ eToken NG-FLASH – одно из решений в области информационной безопасности от компании Aladdin. Он сочетает функционал смарт-карты с возможностью хранения больших пользовательских данных во встроенном модуле flash-памяти. eToken NG-FLASH также обеспечивает возможность загрузки операционной системы компьютера и запуска пользовательских приложений из flash-памяти.

Возможные модификации этого АС: по объему встроенного модуля flash-памяти: 512 МБ; 1, 2 и 4 ГБ; сертифицированная версия (ФСТЭК России); по наличию встроенной радио-метки; по цвету корпуса.

Перейдем теперь к рассмотрению программных средств защиты информации (ПС).

Программные средства (ПС) – это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения.

Программными называются средства защиты данных, функционирующие в составе программного обеспечения. Среди них можно выделить и подробнее рассмотреть следующие: средства архивации данных; антивирусные программы; криптографические средства; средства идентификации и аутентификации пользователей; средства управления доступом; протоколирование и аудит.

Как примеры комбинаций вышеперечисленных мер можно привести ПС: защиту баз данных; защиту операционных систем; защиту информации при работе в компьютерных сетях.

Рассмотрим теперь **средства архивации информации** (СА). Максимальные емкости любых информационных систем ограничены.

Поэтому (а также для целей безопасности) всегда создают резервные копии информации, которые нужно где-то размещать и как-то сохранять. В этих случаях используют программную архивацию.

Архивация – это слияние нескольких файлов и даже каталогов в единый файл – архив, одновременно с сокращением общего объема исходных файлов путем устранения избыточности, но без потерь информации, т.е. с возможностью точного восстановления исходных файлов. Действие большинства средств архивации основано на использовании алгоритмов сжатия, предложенных в 80-х гг. Абрахамом Лемпелем и Якобом Зивом.

Наиболее известны и популярны следующие архивные форматы: ZIP, ARJ для операционных систем DOS и Windows; TAR для операционной системы Unix; межплатформный формат JAR (Java ARchive); RAR – сейчас растет популярность именно этого формата, так как уже разработаны программы, позволяющие использовать его в операционных системах DOS, Windows и Unix.

Пользователю следует лишь выбрать для себя подходящую программу, обеспечивающую работу с выбранным форматом, путем оценки ее характеристик – быстродействия, степени сжатия, совместимости с большим количеством форматов, удобности интерфейса, выбора операционной системы и т.д. Список таких программ очень велик – PKZIP, PKUNZIP, ARJ, RAR, WinZip, WinArj, ZipMagic, WinRar и много других. Большинство из этих программ не надо специально покупать, так как они предлагаются как программы условно-бесплатные (Shareware) или свободного распространения (Freeware). Также очень важно установить постоянный график проведения таких работ по архивации данных или выполнять их после большого обновления данных.

Все большее значение сейчас приобретают **антивирусные программы** (АП). Это программы специально приспособлены для защиты информации от компьютерных вирусов (КВ). Обычно считают, что компьютерный вирус – это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам (т.е. «заражать» их), а также выполнять нежелательные различные действия на компьютере.

Более строго КВ определяют специалисты по компьютерной вирусологии, которые устанавливают, что обязательным свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Следует отметить, что это условие не является достаточным, т.е. окончательным. Вот почему точного определения вируса нет до сих пор, и вряд ли оно появится в обозримом будущем. Следовательно, нет точно определенного закона, по которому безвредные файлы можно отличить от вирусов. Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

Среди КВ обычно выделяют **вредоносные компьютерные вирусы** – как отдельный класс программ, направленных на нарушение работы системы и порчу данных. Среди вирусов выделяют ряд разновидностей. Одни из них постоянно находятся в памяти компьютера, другие производят деструктивные действия разовыми «ударами».

Существует так же целый класс программ, внешне вполне благопристойных, но на самом деле портящих систему. Такие программы называют «троянскими конями». Одним из основных свойств компьютерных вирусов является способность к «размножению», т.е. самораспространению внутри компьютера и компьютерной сети.

С тех пор, как различные офисные прикладные программные средства получили возможность работать со специально для них написанными программами (например, для Microsoft Office можно писать приложения на языке Visual Basic) появилась новая разновидность **вредоносных программ** – макровирусы. Вирусы этого типа распространяются вместе с обычными файлами документов и содержатся внутри них в качестве обычных подпрограмм.

С учетом мощного развития средств коммуникации и резко возросших объемов обмена данными проблема защиты от вирусов становится очень актуальной. Практически с каждым полученным, например, по электронной почте документом может быть получен

макровирус, а каждая запущенная программа может (теоретически) заразить компьютер и сделать систему неработоспособной.

Поэтому среди систем безопасности важнейшим направлением является **борьба с вирусами**. Существует целый ряд средств, специально предназначенных для решения этой задачи. Одни из них запускаются в режиме сканирования и просматривают содержимое жестких дисков и оперативной памяти компьютера на предмет наличия вирусов. Другие же должны быть постоянно запущены и находиться в памяти компьютера. При этом они стараются следить за всеми выполняющимися задачами.

Сейчас на рынке программного обеспечения большую популярность завоевал пакет AVP, разработанный российской лабораторией антивирусных систем Касперского. Это универсальный продукт, имеющий версии под самые различные операционные системы. Также существуют следующие виды**:** Acronis AntiVirus, AhnLab Internet Security, AOL Virus Protection, ArcaVir, Ashampoo AntiMalware, Avast!, Avira AntiVir, A-square anti-malware, BitDefender, CA Antivirus, Clam Antivirus, Command Anti-Malware, Comodo Antivirus, Dr.Web, eScan Antivirus, F-Secure Anti-Virus, G-DATA Antivirus, Graugon Antivirus, IKARUS virus.utilities, Антивирус Касперского, McAfee VirusScan, Microsoft Security Essentials, Moon Secure AV, Multicore antivirus, NOD32, Norman Virus Control, Norton AntiVirus, Outpost Antivirus, Panda и т.д.

Рассмотрим теперь **методы обнаружения и удаления компьютерных вирусов**. Методы противодействия компьютерным вирусам можно разделить на несколько групп: профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения; методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса. **Способы обнаружения и удаления неизвестного вируса** следующие: профилактика заражения компьютера; восстановление пораженных объектов; антивирусные программы.

Профилактика заражения компьютера. Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение некоторых правил, которые позволяют

значительно снизить вероятность заражения вирусом и потери каких-либо данных. Для того чтобы определить основные правила компьютерной гигиены, необходимо выяснить основные пути проникновения вируса в компьютер и компьютерные сети.

Основным **источником вирусов** на сегодняшний день является глобальная сеть Internet. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word. Пользователь зараженного макровирусом редактора, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д. Выводы – следует избегать контактов с подозрительными источниками информации и пользоваться только законными (лицензионными) программными продуктами.

Восстановление пораженных объектов. В большинстве случаев заражения вирусом процедура восстановления зараженных файлов и дисков сводится к запуску подходящего антивируса, способного обезвредить систему. Если же вирус неизвестен ни одному антивирусу, то достаточно отослать зараженный файл фирмам-производителям антивирусов и через некоторое время (обычно – несколько дней или недель) получить лекарство – «update» против вируса. Если же время не ждет, то обезвреживание вируса придется произвести самостоятельно. Для большинства пользователей необходимо иметь резервные копии своей информации. Основная питательная среда для массового распространения вируса в ЭВМ – это: слабая защищенность операционной системы (ОС); наличие разнообразной и довольно полной документации по ОС и «железу», используемой авторами вирусов; широкое распространение этой ОС и этого «железа».

Рассмотрим теперь **криптографические средства защиты информации** (КС), среди которых выделим криптографический способ, архивацию, антивирусный способ и компьютерный способ. Основным механизмом обеспечения информационной безопасности является криптографическая защита информации посредством криптографического **шифрования**.

Криптография – это наука, которая изучает и описывает модель информационной безопасности данных. Криптография открывает

решения многих проблем информационной безопасности сети: аутентификация, конфиденциальность, целостность и контроль взаимодействующих участников. Криптографические методы защиты информации применяются для обработки, хранения и передачи информации на носителях и по сетям связи. Криптографическая защита информации при передаче данных на большие расстояния является единственно надежным способом шифрования.

Термин «шифрование» означает преобразование данных в форму, нечитабельную для человека и программных комплексов без ключа шифрования-расшифровки. Криптографические методы защиты информации дают средства информационной безопасности, поэтому она является частью концепции информационной безопасности.

Криптографическая защита информации (конфиденциальность). Цели защиты информации в итоге сводятся к обеспечению конфиденциальности информации и защите информации в компьютерных системах в процессе передачи информации по сети между пользователями системы.

Защита конфиденциальной информации, основанная на криптографической защите информации, шифрует данные при помощи семейства обратимых преобразований, каждое из которых описывается параметром, именуемым «ключом» и порядком, определяющим очередность применения каждого преобразования.

Важнейшим компонентом криптографического метода защиты информации является ключ, который отвечает за выбор преобразования и порядок его выполнения. **Ключ** – это некоторая последовательность символов, настраивающая шифрующий и дешифрующий алгоритм системы криптографической защиты информации. Каждое такое преобразование однозначно определяется ключом, который определяет криптографический алгоритм, обеспечивающий защиту информации и информационную безопасность информационной системы.

Один и тот же алгоритм криптографической защиты информации может работать в разных режимах, каждый из которых обладает определенными преимуществами и недостатками, влияющими на надежность информационной безопасности.

Защита информации в локальных сетях и технологии защиты информации наряду с конфиденциальностью обязаны обеспечивать и целостность хранения информации. То есть защита информации в локальных сетях должна передавать данные таким образом, чтобы данные сохраняли неизменность в процессе передачи и хранения.

Для того чтобы информационная безопасность обеспечивала целостность хранения и передачи данных, необходима разработка инструментов, обнаруживающих любые искажения исходных данных, для чего к исходной информации придается избыточность.

Информационная безопасность с криптографией решает вопрос целостности путем добавления некой контрольной суммы или проверочной комбинации для вычисления целостности данных. Таким образом, снова модель информационной безопасности является криптографической – зависящей от ключа. По оценке информационной безопасности, основанной на криптографии, зависимость возможности прочтения данных от секретного ключа является наиболее надежным инструментом и даже используется в системах информационной безопасности государства.

Как правило, **аудит информационной безопасности предприятия**, например, информационной безопасности банков, обращает особое внимание на вероятность успешно навязывать искаженную информацию, а криптографическая защита информации позволяет свести эту вероятность к ничтожно малому уровню. Подобная служба информационной безопасности данную вероятность называет мерой имитостойкости шифра, или способностью зашифрованных данных противостоять атаке взломщика.

Защита информации в компьютерных системах от несанкционированного доступа. Для осуществления несанкционированного доступа злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав компьютерных систем. Он осуществляет несанкционированный доступ, используя: знания о компьютерных системах и умения работать с ней; сведения о системе защиты информации; сбои, отказы технических и программных средств; ошибки, небрежность обслуживающего персонала и пользователей.

Для защиты информации от несанкционированного доступа создается система разграничения доступа к информации. Получить несанкционированный доступ к информации при наличии системы разграничения доступа возможно только при сбоях и отказах компьютерных систем, а также используя слабые места в комплексной системе защиты информации. Чтобы использовать слабости в системе защиты, злоумышленник должен знать о них.

Одним из путей добывания информации о недостатках системы защиты является изучение механизмов защиты. Злоумышленник может тестировать систему защиты путем непосредственного контакта с ней. В этом случае велика вероятность обнаружения системой защиты попыток ее тестирования. В результате этого службой безопасности могут быть предприняты дополнительные меры защиты.

Гораздо более привлекательным для злоумышленника является другой подход. Сначала получается копия программного средства системы защиты или техническое средство защиты, а затем производится их исследование в лабораторных условиях.

Кроме того, создание неучтенных копий на съемных носителях информации является одним из распространенных и удобных способов хищения информации. Этим способом осуществляется несанкционированное тиражирование программ. Скрытно получить техническое средство защиты для исследования гораздо сложнее, чем программное, и такая угроза блокируется средствами и методами, обеспечивающими целостность технической структуры компьютерных систем.

Для блокирования несанкционированного исследования и копирования информации компьютерных систем используется комплекс средств и мер защиты, которые объединяются в систему защиты от исследования и копирования информации. Таким образом, система разграничения доступа к информации и система защиты информации могут рассматриваться как подсистемы системы защиты от несанкционированного доступа к информации.

Другие программные средства защиты информации. Выделим среди них межсетевые экраны (также называемые **брандмауэры** или **файрволы** – от нем. brandmauer, англ. firewall – «противопожарная

стена»). С помощью таких экранов между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью.

Более защищенная разновидность метода – это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

Proxy-servers (proxy – доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью – маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях, например, на уровне приложения (вирусы, код Java и JavaScript).

VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.

Подчеркнем, что метод **криптографии** – одно из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Основной элемент криптографии – шифрование (или преобразование данных в нечитабельную форму ключей шифрования-расшифровки). В состав криптографической системы входят: один или несколько алгоритмов шифрования, ключи, используемые этими алгоритмами шифрования, подсистемы управления ключами, незашифрованный и зашифрованный тексты.

При использовании метода криптографии на первом этапе к тексту, который необходимо шифровать, применяются алгоритм шифрования и ключ для получения из него зашифрованного текста. На втором этапе зашифрованный текст передается к месту

назначения, где тот же самый алгоритм используется для его расшифровки.

Ключом называется число, используемое криптографическим алгоритмом для шифрования текста.

В криптографии используется **два метода шифрования** – симметричное и асимметричное. При симметричном шифровании для шифрования и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого они договариваются заранее. Основной недостаток симметричного шифрования состоит в том, что ключ должен быть известен как отправителю, так и получателю, откуда возникает новая проблема безопасной рассылки ключей.

Существует также вариант **симметричного шифрования**, основанный на использовании составных ключей, когда секретный ключ делится на две части, хранящиеся отдельно. Таким образом, каждая часть сама по себе не позволяет выполнить расшифровку.

Асимметричное шифрование характеризуется тем, что при шифровании используются два ключа: первый ключ делается общедоступным (публичным) и используется для шифровки, а второй является закрытым (секретным) и используется для расшифровки Дополнительным методом защиты шифруемых данных и проверки их целостности является цифровая подпись.

Основные выводы о способах использования рассмотренных выше средств, методов и мероприятий защиты, сводится к следующему: наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации; механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы; функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации; необходимо осуществлять постоянный контроль функционирования механизма защиты.

4.2 Ранжирование рисков цифровой экономики

В цифровой экономике все риски и угрозы можно разделить на две группы. Первая группа – это риски и угрозы, относящиеся непосредственно к самим применяемым информационным технологиям. Вторая группа – риски и угрозы, возникающие для объектов и субъектов реальной экономики, связанная с применением в них новых информационных технологий.

Риски и угрозы первой группы достаточно хорошо изучены, защита от них требует всего лишь разумной осторожности, средства защиты и профилактика этих рисков и угроз достаточно эффективны и непрерывно совершенствуются.

Риски и угрозы второй группы нередко проявляются совершено неожиданно, по мере распространения современных информационных технологий на все новые и новые сферы человеческой деятельности; ущербы и потери от них могут быть весьма значительными, поскольку средства защиты обычно запаздывают с их разработкой и внедрением, а о профилактике этих рисков и угроз часто задумываются слишком поздно. По этим причинам риски и угрозы этой группы имеют тенденцию к их долгосрочному воздействию, иногда они на время затихают под воздействием средств борьбы с ними или самопроизвольно, но позже вновь вспыхивают с новой силой.

Различия между рисками и угрозами можно квалифицировать следующим образом: риски возникают во время деятельности и их интенсивность (опасность) прямо зависит от интенсивности деятельности соответствующего вида, а угрозы имеют непрерывный характер и сила их вредоносного воздействия не зависит от действия или бездействия соответствующих субъектов в данной отрасли или в сфере деятельности. В качестве примера рисков можно указать на возможность заражения личного компьютера компьютерными вирусами: если проявлять достаточную осторожность и ограничить свои коммуникации с этого компьютера хорошо известными адресатами, то этот риск становится минимальным. В качестве примера угрозы можно привести радиацию – она нарушает действие информационных систем и аппаратных средств независимо от интенсивности их использования, или даже без такого использования вообще.

Для **определения средств и методов защиты** риски и угрозы следует ранжировать по степени (уровню интенсивности) их опасности. Из практики противодействия этим рискам и угрозам можно определить градацию их интенсивности по пяти уровням, которые целесообразно определить разными цветами: голубой, фиолетовый, желтый, оранжевый, красный.

Самый низкий уровень маркируется кружочком голубого цвета. На этом уровне субъект деятельности и применяемые им информационные технологии могут сталкиваться с проблемами только текущего характера, которые легко разрешаются средствами защиты, штатно встраиваемые в используемые им аппаратные и программные средства цифровизации.

Следующие уровни маркируются звездочками вышеуказанных цветов и степень опасности от этих рисков и угроз показывается количеством этих цветных звездочек, от одной до четырех.

Таким образом, при таком методе маркирования рисков и угроз система их ранжирования включает в себя два **показателя**: показатель их **вероятности** и показатель их **интенсивности**. В качестве частного примера можно привести размещение атомной электростанции (АЭС) в некотором регионе: интенсивность опасности в случае ее разрушения отмечается высшим, красным, цветом, а число этих красных звездочек зависит от природно-климатических условий данного региона.

Так, четыре красные звездочки показывают характер и степень опасности размещения АЭС – для зоны землетрясений, тайфунов, вблизи вулканов, а три красные звездочки и меньше – для всех других регионов.

В случае применения информационных технологий **красный уровень** опасности требует применения особых, разработанных специально для данной ситуации и для данного вида деятельности средств защиты, включая, возможно, и вообще отказ от осуществления такой деятельности.

Далее, если мы вернемся к началу нашего ранжирования, то **фиолетовый уровень** опасности предполагает применение обычных, массового производства, аппаратных средств, хорошо протестированных массовых программных продуктов и стандартных средств защиты от

вирусов. И в зависимости от ущерба, который могут принести неполадки в ходе данного вида деятельности, применяется маркировка от четырех до одной звездочки опасности.

Желтый цвет – цвет тревоги. На этом уровне требуется применение аппаратных средств лучших брендов с функциями дублирования, специализированных для данной отрасли или для данного вида деятельности, программных продуктов и разработка особой системы защиты баз данных от любого внешнего воздействия.

Оранжевый цвет указывает на приближение к красному уровню опасности. На этом уровне наличие возможных рисков и угроз должно учитываться еще до начала соответствующей деятельности и сама конфигурация, состав и объемы этой деятельности должны планироваться, принимая во внимание необходимость постоянного противодействия предсказуемым или вероятным рискам и угрозам.

При оранжевом уровне состав применяемых аппаратных средств и программных продуктов должны определяться с привлечением ведущих консультационных фирм; информационные системы также должны строиться в индивидуальном порядке, силами высокопрофессиональных кадров, а для их защиты должно быть предусмотрено постоянное сопровождение силами известных в этой сфере фирм и компаний.

По своим качественным характеристикам риски – как функциональный, зависимый фактор, связанный с деятельностью в сфере цифровой экономики – **подразделяются** на риски технического и технологического характера, риски программных продуктов, риски от обычных человеческих ошибок, риски от злоупотреблений со стороны собственного персонала и риски от внешних воздействий (со стороны конкурентов, противников и прочих недоброжелателей).

Угрозы – как постоянный фактор неблагоприятного воздействия внешнего и внутреннего характера на применяемые информационные системы – весьма изменчивы и по **объему** и по **степени их опасности**.

В частности, можно выделить угрозы попадания в систему неверной (фэйковой) информации, потери или укрытие важной информации, а также целый ряд возможных конфликтов: между сложившейся у субъекта системой управления и требованиями информационных

технологий, между разными системами ИТ, между управляющими ИТ-системами и человеческим фактором (пример – аварии в авиации), между разными уровнями (иерархиями) в структурах управления.

Нередко имеет место просто неправильное распределение информационных потоков в управляющей системе: когда на одних уровнях этой системы избыток, а на других, наоборот, недостаток информации; когда у лиц, принимающих решения, недостает достоверных данных, позволяющих правильно оценить обстановку и принимать правильные и оправданные складывающейся обстановкой решения.

Следует выделить также угрозы **злонамеренного вмешательства** в информационные системы и базы данных недоброжелателей с внешней стороны – например, иностранное вмешательство в выборы, деятельность рейтинговых фирм, организаций по изучения общественного мнения и т.д.

Особо следует отметить феномен **переполнения систем избыточной информацией,** когда лишняя, ненужная информация поглощает в себе островки необходимой информации и когда управляющие конкретной системой в условиях ограниченного времени реагирования могут принимать неверные и просто фатальные решения.

Интересно, что известный писатель Стивен Кинг заметил эту угрозу еще в 1983 году, когда эра компьютеров еще только начиналась: «В нашем обществе есть проблема информационной перегрузки, информация поступает со всех сторон, льется нам в головы нескончаемым потоком»[9]. Особо заметна в этой сфере деятельность средств массовой информации (СМИ), которые из непроверенного или даже вообще ложного сообщения научились создавать сенсации, сбивающие с толку не только общественное мнение, но и правительства.

В целом, рискам и угрозам в сфере цифровой экономики в последние годы в мире уделяется все большее внимание.

Так, в начале 2020 года международной организацией Global Risks был опубликован доклад о глобальных рисках, которые представляют наибольшую угрозу человечеству на ближайшие десять лет.

[9] Кинг С. Секретные окна. М. 2018, с. 316.

В его подготовке принимали участие 750 экспертов, оценивших воздействия и вероятности 30 распространенных глобальных рисков, а также определивших 13 основных тенденций, которые могут усиливаться в течение 10-летнего периода.

Этот факт наглядно свидетельствует о важности разработки новых методик, методов оценки и предупреждения рисков на всех этапах развития социально-экономических систем в целом и при построении логистической инфраструктуры, сбытовых потоков в частности.

В докладе также подчеркивается, что разрабатываемые подходы по минимизации рисков должны не только базироваться на традиционных методах предупреждения случайных событий, но и применять новейшие достижения в области исследования потоковых процессов, теории нечетких множеств, IT-технологий и т.д.

Вместе с тем уже существуют разработанные общие методики по работе с выявлением рисков и по разработке средств противодействия им, которые можно назвать системами управления рисками или риск-менеджментом системы.

На первом этапе, прежде чем заниматься выбором метода управления риском, необходимо провести **идентификацию, оценить вероятность и последствия каждого вида риска**. Только это позволит выработать систему мер, не допускающих, предотвращающих или снижающих возможный ущерб.

При этом с точки зрения стандартной системы риск-менеджмента, подходить к различным видам рисков следует по-разному. Так, операционные риски и риски ликвидности часто имеют характер проблемы, решаемой построением правильной организационной процедуры с опорой на знания экспертов. А при работе с рыночными и кредитными рисками следует понимать, что управление такими рисками – это более формализуемая и регулярная задача, связанная с математическими оценками, расчетами и процедурами.

В целом на практике обычно выделяют и используют следующие основные **группы методов управления рисками** (воздействия на риск):

- уклонение (избегание) от риска;

- смягчение риска методом его распределения (между разными субъектами);

- торможение риска (с последующим снижением уровня риска);

- перемещение рисков в иную сферу или область деятельности;

- компенсирующие (риск) действия.

Выбор конкретного метода управления является задачей, которую решает риск-менеджмент организации, зависит от стадии жизненного цикла, на которой находится фирма, уровня ее финансового состояния, выбранной стратегии, а также от психологических аспектов – склонности к риску отдельных лиц, принимающих решения, фирмы в целом.

Далее риски группируются по **видам** в зависимости от деятельности предприятия: пожарной опасности, внезапного прекращения энергоснабжения и несчастного случая, технологический, организационно-управленческий, экологический, экономический, материально-технического обеспечения и т.д. После этого производится оценка вероятности наступления того или иного события, возможные потери, определяются методы парирования рисков.

Но все новые риски и все новые угрозы – в связи с бурным развитием информационных технологий и с их буквально взрывным вторжением в повседневную жизнь людей – выходят на свет каждый день и каждый день они ставят перед нами все новые и новые задачи противодействия им.

Сейчас мы все время слышим (и ощущаем на себе их воздействие) об интернете вещей: умных домах, городах и товарах, реклама которых затекает прямо в мозг юзеров; о дистанционной связи с бытовой техникой, криптовалюте, виртуальной и дополненной реальности, голографии и 3D-печати, тотальной роботизации производств, электронном правительстве и вообще об искусственном интеллекте, связанных воедино в виде всемирной сети искусственного разума.

Новые технологии – Нейронет, нейроморфные микрочипы, нейросети, большие данные (Big Data), машинное самообучение, ДНК-, квантовые или оптические компьютеры, электронное распознавание и даже умная пыль – выстраиваются в технологическую основу грядущего. Все это – элементы нашего будущего повседневного мира, ко-

торые стремительно становятся обыденными и необходимыми, каковым за одно поколение стал интернет.

В разработке и реализации IT участвует все большее количество людей по всему миру, также создается много стартапов, некоторые из них становятся мегакорпорациями.

В нашей стране уже взят курс на цифровую экономику, и в целом можно считать, что российское общество в настоящее время живет в цифровой «системе координат».

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1. Структура и основные функции программно-аппаратных комплексов защиты информации.
2. Состав и практическое использование аппаратных (технических) средств информационной защиты.
3. Место и роль программного обеспечения электронно-вычислительных машин и информационно-коммуникативных сетей в системе информационной безопасности.
4. Комплекс мероприятий по защите информации в условиях предприятия (организации).