ГЛАВА 4. ЦИФРОВАЯ ГРАМОТНОСТЬ И БЕЗОПАСНОСТЬ

§ 1. Анализ и управление рисками в сфере информационной безопасности

В настоящее время информация очень часто рассматривается как наиболее ценный ресурс. Это неудивительно, так как в современном компьютеризированном мире наиболее эффективные конкурентные преимущества фирма может получить в основном за счет обладания уникальной информацией, будь то новейшие технологические разработки, необходимые для успеха на развивающемся рынке мобильных устройств, или данные о предпочтениях интернет-пользователей, имеющие огромную ценность для эффективной целевой рекламы. Кроме того, информация ограниченного доступа (например, персональные данные клиентов) всегда представляла ценность для её обладателей и вызывала интерес со стороны злоумышленников.

Ещё одной причиной актуальности проблемы обеспечения информационной безопасности является повсеместное использование автоматизированных средств хранения, передачи и обработки информации.

Именно поэтому **информационной безопасности (ИБ)** в последнее время уделяется все больше внимания: высший менеджмент предприятий различных сфер деятельности готов тратить все больше сил и средств на создание и развитие системы защиты информации, а также системы менеджмента ИБ. Стоит заметить, что формирование режима информационной безопасности является комплексной задачей и осуществляется на трёх уровнях: законодательно-правовом, административном (организационном) и программно-техническом, поэтому для достижения поставленной цели требуется большое количество материальных и человеческих ресурсов.

Отсюда понятно, почему сейчас анализу рисков информационной безопасности уделяется все больше внимания. Этому есть несколько основных причин: безостановочный рост использования информационных технологий в процессе деятельности практически любой современной организации, увеличение ценности информации, обрабатывающейся и генерирующейся в процессе работы компании, а также интеграция различных информационных продуктов с целью покрытия всех нужд фирмы.

Теперь рассмотрим некоторые основные понятия и определения, необходимые для изучения этой темы.

Начнем с понятия «**Информационная безопасность**» (ИБ), под которой пронимается сохранение конфиденциальности, целостности и доступности информации.

Конфиденциальность – характеристика, определяющая, что информация не может быть доступной или раскрытой для неавторизованного на то лица.

При этом **доступность информации** определяется как доступность и используемость данных по запросу со стороны авторизованного логического объекта.

Целостность можно определить как свойство сохранения правильности и полноты информации.

Далее дадим также определения ситуаций, связанных с нарушением информационной безопасности.

Так, «**событие информационной безопасности**» определим как идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности или аварию защитных мер (средств), а также возникновение ранее не известной ситуации, которая может быть связана с безопасностью.

Инцидент информационной безопасности – одно или серия нежелательных или неожиданных событий информационной безопасности, которые имеют значительную вероятность компрометации бизнес-операции и угрожают информационной безопасности.

Система информационной безопасности (СИБ) – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Система менеджмента информационной безопасности (СМИБ) – та часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании информационной безопасности.

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему.

Уязвимость ИС – это так называемое «слабое место» в информационной системе, которое является основанием для возникновения угрозы со стороны злоумышленников.

Активы – все, что имеет ценность для организации. В информационной системе главным активом является сама информация – базы данных и другая ценная для организации информация, хранящаяся в цифровой форме.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации, находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Особого внимания относительно рисков информационной безопасности заслуживает банковская сфера, так как стоимость информации в компаниях, работающих в данной области, ещё выше за счёт превалирования персональных данных клиентов, обладание которыми даёт возможность получить несанкционированный доступ к финансовым ресурсам.

Кроме того, существует такое понятие, как банковская тайна, суть которого заключается в обязанности каждого банка (или иной кредитной организации) защищать сведения о вкладах и счетах своих клиентов и корреспондентов, банковских операциях по счетам и сделках в интересах клиента, а также сведения клиентов, разглашение которых может нарушить право последних на неприкосновенность частной жизни (ФЗ «О банках и банковской деятельности»).

Таким образом, информация, задействованная в работе коммерческих банков, нуждается в особой защите от потери ее свойств, а именно конфиденциальности, целостности и доступности. В частности, особое внимание должно уделяться поиску уязвимостей в системе защиты информации и анализу и оценке рисков всего контура информационной безопасности.

Однако на данный момент не существует стандартизированной методики анализа и оценки рисков информационной безопасности для кредитных организаций, обязательной для применения банками России. Все разработанные и активно использующиеся методики являются довольно общими для организаций, работающих в различных секторах экономики, они не учитывают особенностей банковского законодательства и специфики деятельности кредитных организаций.

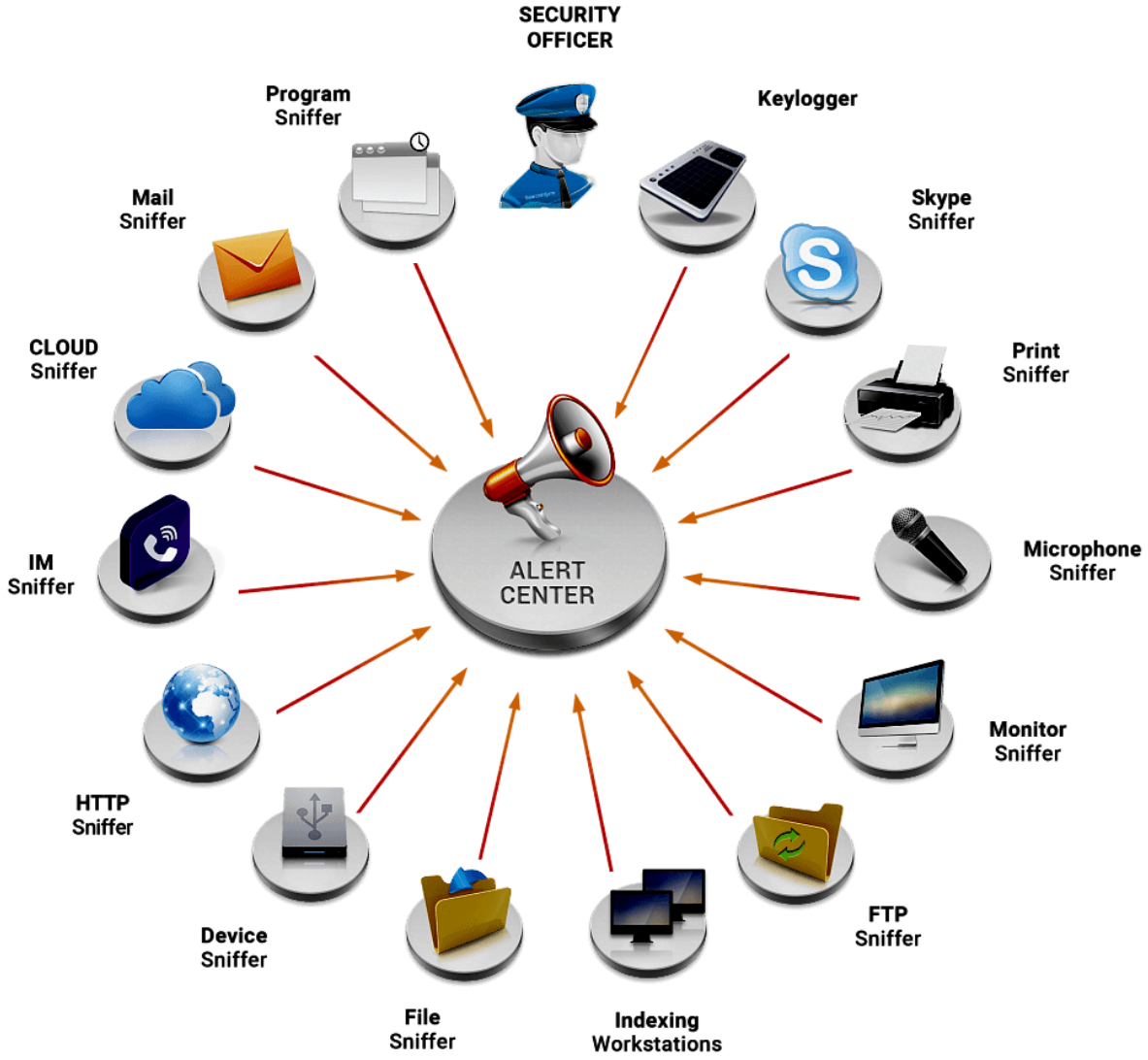

Рис. 26. Контур информационной безопасности

Между тем, изучение современных методик анализа и управления рисками, связанными с информационной безопасностью (ИБ), является необходимостью для любого пользователя информационных технологий, и не только в сфере банковской деятельности. При этом под рисками в сфере ИБ следует понимать потенциальную возможность понести убытки и потери из-за нарушения безопасности информационной системы (ИС). При этом отметим, что понятие риска отличается от понятия угрозы именно тем, что риск отличает

наличие количественной оценки возможных потерь и оценки вероятности наступления нежелательного события.

Как известно, для любого проекта, требующего финансовых затрат на его реализацию, весьма желательно уже на начальной стадии определить, что следует считать положительным результатом проекта. Для задач, связанных с обеспечением ИБ, это тем более важно и актуально.

На практике наибольшее распространение получили два **подхода** к обоснованию проекта подсистемы обеспечения безопасности.

Первый из них основан на проверке соответствия уровня защищенности ИС требованиям одного из стандартов в области информационной безопасности. Это может быть класс защищенности в соответствии с требованиями руководящих документов Гостехкомиссии РФ (сейчас это ФСТЭК России), профиль защиты, разработанный в соответствии со стандартом ISO-15408 (см. раздел 1.5), или какой-либо другой набор требований. Тогда критерий достижения цели в области безопасности – это выполнение заданного набора требований. Критерий эффективности – минимальные суммарные затраты на выполнение поставленных функциональных требований.

При этом основной недостаток данного подхода заключается в том, что в случае, когда требуемый уровень защищенности жестко не задан (например, через законодательные требования), определить «наиболее эффективный» уровень защищенности ИС достаточно сложно.

Второй подход к построению системы обеспечения ИБ связан с оценкой и управлением рисками. Изначально он произошел из принципа «разумной достаточности», примененного к сфере обеспечения ИБ. Этот принцип был описан следующим набором утверждений: абсолютно непреодолимую систему защиты создать невозмож-

но; необходимо соблюдать баланс между затратами на защиту и получаемым эффектом, в т.ч. и экономическим, заключающимся в снижении потерь от нарушений безопасности; стоимость средств защиты не должна превышать стоимости защищаемой информации (или других ресурсов – аппаратных, программных); затраты нарушителя на несанкционированный доступ к информации должны превышать тот эффект, который он получит, осуществив подобный доступ.

К сожалению, на практике точные зависимости между затратами и уровнем защищенности определить не представляется возможным, поэтому аналитический метод определения минимальных затрат в представленном виде неприменим. Поэтому, для того чтобы перейти к рассмотрению вопросов описания риска, введем еще одно определение.

Ресурсом или *активом* будем называть именованный элемент ИС, имеющий (материальную) ценность и подлежащий защите.

Тогда риск может быть идентифицирован следующим набором параметров: угроза, с возможной реализацией которой связан данный риск; ресурс, в отношении которого может быть реализована угроза (ресурс может быть информационный, аппаратный, программный и т.д.); уязвимость, через которую может быть реализована данная угроза в отношении данного ресурса.

Практическое задание

1. Проанализировать систему информационной безопасности конкретного предприятия (рассмотреть имеющиеся средства и методы защиты информации).

2. Произвести оценку рисков существующей системы безопасности, результаты свести в таблицу:

Наименование угрозы	Вероятность наступления	Ущерб от реализации	Риск
Стихийные бедствия, аварии, пожары и пр.	3	3	9
Непреднамеренные ошибки пользователей	2	2	4
Перебои электропитания	1	2	2
Вредоносное программное обеспечение	2	3	6
Халатность пользователей	3	2	6
Другое			
Сумма рисков:			27

Проставить в таблице коэффициент вероятности наступления и коэффициент ущерба от реализации угрозы по 3-хбалльной шкале. Произведение этих составляющих позволит определить риск. Рассчитать общую сумму рисков. На основе полученных данных выделить три типа риска: низкий (1, 2), средний (3, 4), высокий (6, 9). Построить диаграмму оценки рисков по категориям. Сделать выводы.

3. Предложить средства улучшения системы информационной безопасности предприятия, охарактеризовать каждое из них. Провести сравнительный анализ этих средств с их аналогами (допускается использование данных социологических опросов; характеристики технических средств должны соответствовать реальным).

4. Провести оценку рисков разработанной системы безопасности и свести данные в таблицу 2 – Оценка рисков разработанной системы безопасности, аналогичную таблице 1. Построить диаграмму количества рисков после принятия разработанной политики безопасности. Сделать выводы.

5. Сделать общий вывод (можно ли считать разработанную систему безопасности эффективной, ответ аргументировать).

Важно также определить то, как мы узнаем, что нежелательное событие произошло. Поэтому в процессе описания рисков обычно также указывают события – *«триггеры»,* являющиеся идентификаторами рисков, произошедших или ожидающихся в скором времени

(например, увеличение время отклика web-сервера может свидетельствовать о производимой на него одной из разновидностей атак на «отказ в обслуживании»).

Исходя из сказанного выше, в процессе оценки риска надо оценить стоимость ущерба и частоту возникновения нежелательных событий и вероятность того, что подобное событие нанесет урон ресурсу. Размер ущерба от реализации угрозы в отношении ресурса зависит от стоимости ресурса, который подвергается риску, и степени разрушительности воздействия па ресурс, выражаемой в виде коэффициента разрушительности.

Далее необходимо оценить частоту возникновения рассматриваемого нежелательного события (за какой-то фиксированный период времени, например, за год) и вероятность успешной реализации угрозы. Затем ожидаемый ущерб сравнивается с затратами на меры и средства защиты, после чего принимается решение в отношении данного риска.

Он может быть: принят; снижен (например, за счет внедрения средств и механизмов защиты, уменьшающих вероятность реализации угрозы или коэффициент разрушительности); устранен (за счет отказа от использования подверженного угрозе ресурса); или перенесен на другое лицо (например, застрахован, в результате чего в случае реализации угрозы безопасности потери будет нести страховая компания, а не владелец ИС).

Как известно, **анализ и оценка рисков** ИБ проводятся для получения следующей информации:

– какие риски информационной безопасности существуют в организации; какова вероятность их реализации;

– какой ущерб будет нанесен в результате их реализации;

– какие риски компания может принять (на основе критериев

принятия риска);

– какие средства защиты являются наиболее адекватными для борьбы с той или иной уязвимостью в СИБ;

– какой объем денежных средств должен быть в резерве на случай возникновения инцидента информационной безопасности, и т.д.

При этом есть несколько стандартов, в которых описываются требования к построению систем менеджмента информационной безопасности. Это такие документы, как ГОСТ Р ИСО/МЭК 27001[4] и ГОСТ Р ИСО/МЭК 17799. В обоих из них содержится информация о правилах и порядке проведения анализа и оценки рисков информационной безопасности.

Так, по ГОСТ Р ИСО/МЭК 27001 порядок работы с рисками следующий: идентификация рисков – идентифицировать активы, относящиеся к области применения СМИБ, и определить собственников этих активов; идентифицировать угрозы этим активам; идентифицировать уязвимости, которые могут быть использованы этими угрозами; идентифицировать возможные воздействия, которые могут привести к утрате конфиденциальности, целостности и доступности активов.

Для анализа и оценки риска необходимо: оценить ущерб бизнесу, который может быть нанесен в результате нарушения безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности или доступности активов; оценить реальную вероятность возникновения такого нарушения безопасности в свете превалирующих угроз и уязвимостей, воздействия на соответствующие активы, а также применяемые меры контроля; оценить уровни рисков; определить, является ли риск приемлемым или требуется обработка риска с использованием определенных критериев.

Очевидно, что данные рекомендации – это примерный и очень

общий план действий по управлению рисками информационной безопасности, не позволяющий, следуя ему, эффективно оценить риски ИБ в крупной компании. Так как государственных стандартов недостаточно, широкое применение приобретают методики, разрабатываемые частными компаниями, такие как Lifecycle Security или методика Microsoft.

Здесь также стоит упомянуть о существовании средства оценки безопасности «Microsoft Security Assessment Tool (MSAT)», который представляет собой бесплатное программное обеспечение, позволяющее «оценить уязвимости в ИТ-средах, предоставить список расставленных по приоритетам проблем и список рекомендаций по минимизации этих угроз».

Рассмотрим **порядок применения программы управления рисками** в системе информационной безопасности по методике Microsoft.

Вначале отметим, что этапы качественной оценки рисков во всех методиках примерно одинаковы: выявление рисков ИБ, определение вероятности возникновения каждого из них, определение стоимости активов, которые пострадают от реализации конкретного риска, а также распределение описанных рисков на группы в зависимости от ранее оговоренных критериев значительности риска, а также возможности его принятия. Так и в данной методике на начальном этапе рискам присваиваются значения в соответствии со шкалой: «высокий» (красная область), «существенный» (жёлтая область), «умеренный» (синяя область) и «незначительный» (зеленая область). После этого, при выявленных наиболее существенных рисках и подсчете финансовых показателей, проводится количественная оценка.

При этом для проведения эффективной оценки требуется собрать самые актуальные данные об активах организации, угрозах

безопасности, уязвимостях, текущей среде контроля и предлагаемых элементах контроля. Далее проводится сложный и многоступенчатый процесс анализа и оценки рисков, в результате которого владельцы бизнеса получают информацию не только о существующих рисках, вероятностях их реализации, уровнях влияния на деятельность компании, но и оценку ожидаемого годового ущерба (ALE).

Процесс анализа информационной сети на наличие в ней уязвимостей против возможных угроз и к возможным рискам осуществляется с помощью ответов на более чем 200 вопросов, «охватывающих инфраструктуру, приложения, операции и персонал».

Первая серия вопросов предназначена для определения бизнес-модели компании, на основе полученных ответов средство создает «профиль бизнес-риска (BRP)». По результатам ответа на вторую серию вопросов составляется список защитных мер, внедренных компанией с течением времени.

В совокупности эти меры безопасности «образуют уровни защиты, предоставляя большую защищенность от угроз безопасности и конкретных уязвимостей». Сумма уровней, образующих «комбинированную систему глубокой защиты», называется «индексом глубокой защиты (DiDI)».

После этого BRP и DiDI сравниваются между собой для измерения распределения угроз по областям анализа – инфраструктуре, приложениям, операциям и людям. Полученная оценка предназначена для использования в организациях среднего размера, «содержащих от 50 до 1500 настольных систем».

В результате её использования менеджмент компании получает общую информацию о состоянии системы защиты информации предприятия, охватывая большинство «областей потенциального риска», но описываемое средство не предусмотрено для предоставления «глубокого анализа конкретных технологий или процессов».

Следующая методика «CCTA Risk Analysis and Management Method (CRAMM)» – одна из первых методик анализа рисков в сфере информационной безопасности. В основе **метода CRAMM** лежит комплексный подход, сочетающий процедуры количественной и качественной оценки рисков. Исследование информационной безопасности системы с помощью CRAMM может проводиться двумя способами, преследующими две качественно разные цели: обеспечение базового уровня ИБ и проведение полного анализа рисков. От того, какая задача стоит перед специалистами по оценке рисков, зависит количество проводимых этапов работы.

Перечислим все возможности данной методики, делая акцент на обстоятельствах применения той или иной процедуры анализа. **Первая стадия** является подготовительной и обязательной при постановке любой из двух возможных целей исследования информационной безопасности системы. Во время данного этапа формально определяются границы рассматриваемой информационной системы, ее основные функции, категории пользователей и персонала, принимающего участие в исследовании.

На **второй стадии** проводится анализ всего, что касается выявления и определения ценности ресурсов рассматриваемой системы: проводится идентификация физических, программных и информационных ресурсов, находящихся внутри границ системы, а затем производится распределение их на заранее выделенные классы. В результате заказчик имеет хорошее представление о состоянии системы и может принять решение о необходимости проведения полного анализа рисков. При условии, что обеспечения базового уровня ИБ клиенту недостаточно, строится модель информационной системы с позиции ИБ, которая позволит выделить наиболее критичные элементы.

На **третьей стадии**, которая проводится только в том случае, если необходимо проведение полного анализа рисков, рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. На данном этапе оценивается влияние определенных групп ресурсов на работоспособность пользовательских сервисов, определяется текущий уровень угроз и уязвимостей, вычисляются уровни рисков и проводится анализ результатов. В итоге заказчик получает идентифицированные и оцененные уровни рисков ИБ для исследуемой системы.

На **четвертой стадии** для каждой группы ресурсов и каждого из 36 типов угроз программное обеспечение CRAMM составляет список вопросов, предполагающих однозначный ответ.

Как и в случае с методикой компании Microsoft, в CRAMM проводится качественная оценка риска путем отнесения уровней угроз к той или иной категории в зависимости от полученных ответов. Всего в данной методике есть пять категорий уровней угроз: «очень высокий», «высокий», «средний», «низкий» и «очень низкий». В свою очередь, уровень уязвимости ресурса оценивается, в зависимости от ответов, как «высокий», «средний» и «низкий».

На основе данной информации, а также размеров ожидаемых финансовых потерь, рассчитываются уровни рисков по шкале от 1 до 7, объединенные в матрице оценки риска.

При этом следует отметить, что метод CRAMM по праву может быть отнесен к методикам, использующим как качественный, так и количественный подходы к анализу рисков информационной безопасности, так как в процессе проведения оценки учитывается уровень ожидаемых финансовых потерь от реализации риска, а результаты предоставляются в баллах по шкале от 1 до 7. Этот факт значительно повышает рейтинг методики CRAMM в глазах специалистов в данной предметной области.

На последней стадии исследования, носящей название «Управление рисками», производится выбор адекватных элементов контроля: программное обеспечение CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням, из которых выбирается оптимальный вариант системы безопасности, удовлетворяющий требованиям заказчика.

Методика «Facilitated Risk Analysis Process (FRAP)» – это модель построения системы защиты информации, включающая в себя качественный анализ рисков. Приведем предусмотренные в этой методике основные этапы оценки рисков.

На первом этапе, с опорой на данные опросов, техническую документацию, автоматизированный анализ сетей, составляется список находящихся в зоне риска активов.

На следующем этапе проводится идентификация угроз. При составлении списка угроз могут использоваться следующие различающиеся методы.

Конвенциональный (обычный) метод. В этом случае эксперты составляют перечни (checklists) потенциальных угроз, из которых впоследствии выбираются наиболее актуальные для данной системы.

Статистический метод. При этом методе проводится анализ статистики происшествий, связанных с информационной безопасностью данной ИС и подобных ей, и оценивается их средняя частота, после чего производится оценка точек риска.

Метод «мозгового штурма», проводимый сотрудниками компании. Отличие от первого метода в том, что он проводится без привлечения внешних экспертов.

Далее, после составления списка потенциальных угроз, производится сбор статистики по каждому случаю возникновения риска: частоте той или иной ситуации, а также по уровню претерпеваемого

ущерба. Опираясь на эти значения, эксперты оценивают уровень угрозы по обоим параметрам: вероятности возникновения угрозы (High Probability, Medium Probability and Low Probability) и ущерба от нее (High Impact, Medium Impact and Low Impact).

Затем, в соответствии с правилом, задаваемым матрицей рисков, определяется оценка уровня риска:

– наивысший уровень, уровень A – направленные на элиминацию угрозы меры (например, внедрение СЗИ) должны быть предприняты немедленно и в обязательном порядке;

– высокий уровень, уровень B – необходимо предпринять меры, направленные на снижение риска;

– средний уровень, уровень C – необходим мониторинг ситуации;

– низкий уровень, уровень D – никаких действий в данный момент предпринимать не требуется.

После того как угрозы были идентифицированы и относительные риски оценены, следует составить план действий, позволяющий устранить риск или уменьшить его до приемлемого уровня.

По окончании оценки рисков результаты должны быть подробно документированы и переведены в стандартизованный формат. Эти данные могут быть использованы при планировании дальнейших процедур в области обеспечения безопасности, бюджета, выделяемого на эти процедуры, и т.д.

Программа Risk Advisor – это программный продукт, разработанный компанией MethodWare, в котором реализована методика, «позволяющая задать модель информационной системы с позиции информационной безопасности, идентифицировать риски, угрозы, потери в результате инцидентов». При работе с этой программой следует реализовать пять основных этапов работы:

Описание контекста. В первую очередь необходимо создать общую схему внешних и внутренних информационных контактов организации. Эта модель строится в нескольких измерениях и задается следующими параметрами: стратегическим, организационным, бизнес-целями, управлением рисками, критериями. Картина общего контекста с точки зрения стратегии описывает сильные и слабые стороны организации в плане внешних контактов. Здесь производится классификация угроз, связанных с отношениями с партнерами, оцениваются риски, сопряженные с различными вариантами развития внешних связей организации. Описание контекста в организационном измерении включает в себя картину отношений внутри организации, стратегию развития и внутреннюю политику. Схема управления рисками включает в себя концепцию информационной безопасности. Наконец, в контексте бизнес-целей и критериев оценки описываются, как следует из названия, ключевые бизнес-цели и качественные и количественные критерии, с опорой на которые производится управление рисками.

Описание рисков. Для того чтобы облегчить и стандартизировать процесс принятия решений, связанных с управлением рисками, данные по ним необходимо стандартизировать. В разных моделях используются разные шаблоны для формализации имеющейся информации. В описываемой нами методике задается матрица рисков, в которой учитываются не только собственные параметры этих рисков, но и информация об их связях с остальными элементами общей системы. Следует отметить, что риски оцениваются здесь по качественной, а не количественной шкале, и делятся всего на две категории: приемлемые и, соответственно, неприемлемые. После этой оценки производится выбор контрмер и анализ стоимости и эффективности выбранных средств защиты.

Описание угроз. Прежде всего, составляется общий список угроз. Затем они классифицируются по качественной шкале, описы-

ваются взаимосвязи между различными угрозами и связи типа «угроза – риск».

Описание потерь. На этом этапе описываются события, связанные с инцидентами информационной безопасности, после чего оцениваются риски, вызванные этими событиями.

Анализ результатов. После построения модели формируется детальный отчет (состоящий более чем из 100 разделов). Агрегированные описания представляются потребителю в виде графа рисков.

Компания RiskWatch, также как и Microsoft, разработала собственную методику анализа и оценки рисков, которая реализуется в ряде их программных средств.

В **методе RiskWatch** в качестве критериев для оценки и управления рисками используются ожидаемые годовые потери (Annual Loss Expectancy, ALE) и оценка возврата инвестиций (Return on Investment, ROI). Методика RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. Процесс анализа рисков состоит из четырех этапов.

На первом этапе, являющемся, по сути, подготовительным, определяется предмет исследования: дается описание типа организации, состава исследуемой системы, базовых требований в области информационной безопасности и т.д. Программное обеспечение RiskWatch предлагает широкий выбор всевозможных категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты, из которых аналитик выбирает только те, что реально присутствуют в исследуемой системе. Кроме того, есть возможность добавления новых элементов и корректировка уже существующих описаний.

На втором этапе производится более детальное описание системы (какие ресурсы в ней присутствуют, какие типы потерь могут

иметь место при реализации риска и какие классы инцидентов можно выделить «путём сопоставления категории потерь и категории ресурсов»). Есть два варианта ввода данных: вручную или путём импорта из отчетов, сгенерированных в процессе анализа компьютерной сети на наличие в ней уязвимостей. Для выявления возможных слабых мест системы используется опросник, в котором предлагается ответить более чем на 600 вопросов, связанных с категориями ресурсов. В связи с тем, что компании из разных сфер деятельности имеют свои исключительные особенности, а также учитывая быстро развивающийся рынок информационных технологий, кажется очень разумным и удобным наличие возможности корректировки вопросов и исключение/добавление новых. Далее определяется частота реализации каждой из присутствующих в системе угроз, уровень уязвимости и ценность ресурсов. На основе данной информации рассчитывается эффективность использования тех или иных элементов контроля информационной безопасности.

На третьем этапе производится количественная оценка риска. Первым делом определяется взаимосвязь между ресурсами, потерями, угрозами и уязвимостями, определенными в процессе проведения первых двух этапов работы. Кроме того моделируются сценарии «что если…», в которых аналогичные ситуации рассматриваются с учетом внедрения средств защиты. Путём сравнения ожидаемых потерь при условии использования элементов контроля и без них можно оценить, насколько эффективным будет внедрение тех или иных защитных мер.

На последнем этапе генерируются отчёты разных видов: «краткие итоги, полные и краткие отчеты об элементах, описанных на стадиях 1 и 2, отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз, отчет об угрозах и мерах противодействия, отчет о результатах аудита безопасности.

Таким образом, применение этой программы позволяет не только оценить риски, которые на данный момент существуют у предприятия, но и выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия. Кроме того, описываемое программное обеспечение может являться удобной основой для разработки собственного, максимально подходящего для предприятий конкретного типа (например, кредитных организаций), средства анализа и оценки рисков информационной безопасности.

Отметим также **ГРИФ** – российское комплексное средство анализа и управления рисками информационной системы организации, разработанное компанией Digital Security. Принцип работы данного программного обеспечения основан на двух концептуально разных подходах к оценке рисков информационной безопасности, получивших названия «модель информационных потоков» и «модель угроз и уязвимостей». Рассмотрим каждый из алгоритмов по отдельности.

«Модель информационных потоков» характеризуется тем, что в основе алгоритма анализа и оценки рисков лежит построение модели информационной системы организации. Расчет значений рисков базируется на информации о средствах защиты ресурсов с ценной информацией, взаимосвязях ресурсов между собой, влиянии прав доступа групп пользователей и организационных мерах противодействия.

На первом этапе необходимо подготовить полное описание архитектуры исследуемой сети, включающее информацию о ценных ресурсах, их взаимосвязях, группах пользователей, средствах защиты информации и др. Исходя из введенных данных, можно построить полную модель информационной системы компании, на основе

которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Далее оценка риска производится отдельно по каждой связи «группа пользователей – информация» по трем типам угроз: конфиденциальность, целостность и доступность (при этом для первых двух типов результат рассчитывается в процентах, а для последнего – в часах простоя). Ущерб от реализации разных видов угроз тоже задается отдельно, т.к. оценить комплексные потери не всегда возможно.

Ключевыми критериями, от которых зависит вероятность реализации той или иной угрозы, являются виды (локальный и/или удаленный) и права (чтение, запись, удаление) доступа пользователей к ресурсам, наличие доступа в интернет, количество человек в группе, использование антивирусного ПО, криптографических средств защиты (особенно значимо для дистанционного доступа) и т.д.

На этом же этапе определяются средства защиты информации и рассчитываются коэффициенты локальной защищенности информации на ресурсе, удаленной защищенности информации на ресурсе и локальной защищенности рабочего места группы пользователей. Минимальный коэффициент отражает реальный уровень защиты ресурса, т.к. указывает на наиболее уязвимое место в информационной системе. Для того чтобы получить итоговую вероятность реализации угрозы, полученный показатель необходимо умножить на базовую вероятность реализации угрозы ИБ, которая рассчитывается на основе метода экспертных оценок.

На последнем этапе значение полученной итоговой вероятности умножается на величину ущерба от реализации угрозы и рассчитывается риск угрозы информационной безопасности для связи «вид информации – группа пользователей». Алгоритм расчета величины риска по угрозе «отказ в обслуживании» имеет незначительные от-

личия, связанные в основном с единицами измерения.

В результате работы использования указанного алгоритма пользователь программы получает следующую информацию: риск реализации по трем базовым угрозам для вида информации, риск реализации по трем базовым угрозам для ресурса, риск реализации суммарно по всем угрозам для ресурса, риск реализации по трем базовым угрозам для информационной системы, риск реализации по всем угрозам для информационной системы, риск реализации по всем угрозам для информационной системы после задания контрмер, эффективность контрмеры, эффективность комплекса контрмер.

«**Модель анализа угроз и уязвимостей**» описывает ещё один подход к анализу и оценке рисков информационной безопасности. В качестве входной информации выступает перечень ресурсов, содержащих ценную информацию, описание угроз, воздействующих на каждый ресурс, и уязвимостей, через которые возможна реализация вышеупомянутых угроз. Для каждого из видов исходных данных (кроме уязвимостей) указывается степень критичности. Также вводится вероятность реализации той или иной угрозы.

Этот алгоритм может работать в двух режимах: рассчитывая вероятность реализации одной базовой угрозы или распределяя оценки по трём базовым типам угроз. Перечислим **этапы** метода в общем виде для обоих режимов.

1. Рассчитывается уровень угрозы по конкретной уязвимости на основе критичности и вероятности реализации угрозы через данную уязвимость.

2. Уровень угрозы по всем уязвимостям рассчитывается путем суммирования уровней угроз через конкретные уязвимости.

3. Рассчитывается общий уровень угроз по ресурсу.

4. Рассчитывается риск по ресурсу.

5. Рассчитывается риск по информационной системе.

Алгоритм анализа и оценки рисков ГРИФ – это образец методики, которая учитывает особенности структуры компании заказчика, используя два разных подхода к расчету величин рисков. Каждый из этих двух методов может быть более эффективен в случае с одной фирмой и менее эффективен в ситуации с другой. Таким образом, методика ГРИФ исключает возможность использования неподходящего алгоритма расчета уровня риска, гарантируя достижения оптимального результата.

Очевидно, что среди описанных в данной работе методик нет идеального варианта, так как ни одна компания-разработчик не ставила своей целью создание алгоритма анализа и оценки рисков ИБ для предприятий какой-либо конкретной сферы.

Наоборот, более логичным является разработка универсального средства для решения проблем информационной безопасности предприятия, которое позволило бы получить максимальную выгоду от его продажи как можно большему числу фирм-клиентов.

Существуют также и специальные методики, разрабатываемые применительно для отдельных отраслей и секторов экономики. Так, в банковской сфере существует особая методика анализа и оценки рисков ИБ в организациях банковской системы РФ, разработанная в 2009 году Банком России, однако она носит лишь рекомендательный характер.

Поэтому и до сегодняшнего времени есть и остается потребность в разработке эталонной методики анализа и оценки рисков информационной безопасности в банковской сфере на основе существующих стандартов и методик построения системы защиты информации на предприятии. Кроме того, процесс анализа и оценки рисков информационной безопасности необходимо рассматривать в контексте разработки системы управления информационной без-

опасностью организации, так как анализ рисков сам по себе не принесет компании желаемого результата, а именно минимизации этих рисков и сокращения ожидаемых потерь от их реализации.

§ 2. Программно-аппаратные средства 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 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 незаконное 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 вещных 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 позволяющих 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.

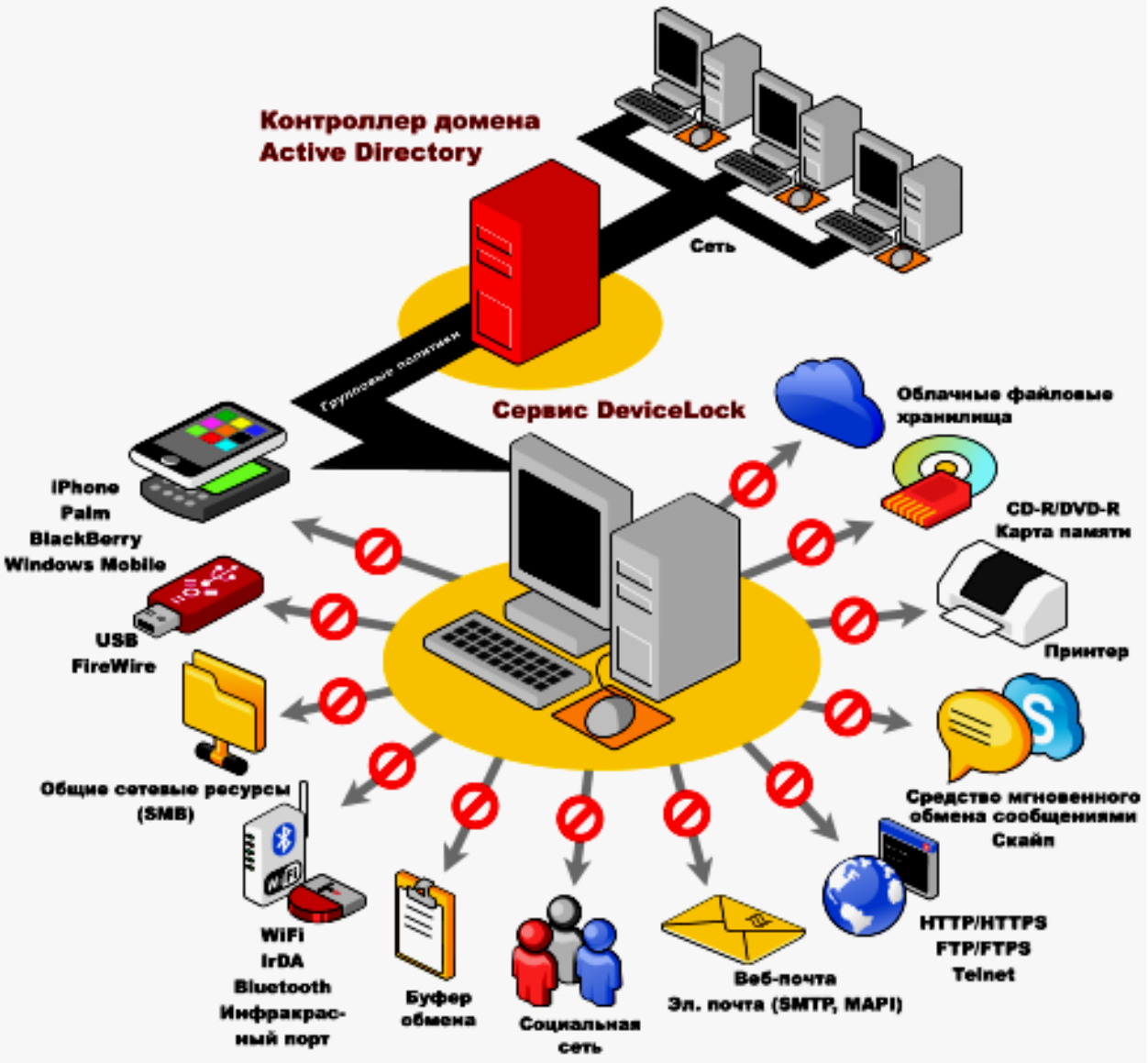

Рис. 27. Аппаратные и программные средства защиты информации

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** 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) 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 видеонаблюдения; 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 (несанкционированному доступу) 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 техвозможностям средства защиты информации могут быть общего на значения, рассчитанные на использование непрофессионалами с целью получения общих оценок, и профессиональные комплексы, позволяющие проводить тщательный поиск, обнаружение и измерения 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 злоумышленниками средств НСД. 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 дорога 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 реализа-

ции сетей хранения наряду с популярной технологией Fiber Channel в последнее время все чаще используются устройства iSCSI.

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 не более 5 минут простоя информационной системы по любой причине.

Удачным сочетанием большой емкости, высокой скорости и приемлемой стоимости в настоящее время являются решения с использованием накопителей Serial ATA и SATA 2.

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 защищённого 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 объёмов пользовательских данных во встроенном

модуле. 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 объёму 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 огра-

ничены. Поэтому – а также и 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). Эти 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 различные нежелательные 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 «хорошие» 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. Некоторые из них постоянно находятся в памяти компьютера, некоторые производят деструктивные действия разовыми «ударами».

Существует также 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. Некоторые из них запускаются в режиме сканирования и просматривают содержимое жестких дисков и оперативной памяти компьютера на предмет наличия вирусов. Некоторые 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 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.

Покажем 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.

Практическое задание

1. Уясните, какая антивирусная программа установлена на вашем ПК.

2. Откройте программу Antivirus и изучите окно программы.

3. Почитайте информацию на вкладках: Состояние защиты, Обновление, Настройка, Служебные программы, Справка и поддержка.

4. Посмотрите на вкладке Настройка, все ли опции включены: Защита в режиме реального времени, Защита электронной почты, Защита доступа в интернет.

5. Включите вкладку Сканирование ПК. Выберите выборочное сканирование. Просканируйте локальный диск С.

6. Пока идёт сканирование, изучите содержимое вкладки Служебные программы. Какие файлы были помещены на карантин?

7. После окончания сканирования локального диска просканируйте свою флэшку. Результаты сканирования диска и дискеты зафиксируйте.

8. В разделе Справочной системы программы найдите информацию о том, какие уровни очистки поддерживает программа.

9. Изучите раздел Справка.

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 небольшого числа правил, которое позволяет 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, не читабельную 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 информации 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 лимитостойкости шифра, или способностью зашифрованных данных противостоять атаке взломщика.

Защита информации в КС от несанкционированного доступа. Для осуществления несанкционированного доступа злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав КС. Он осуществляет несанкционированный доступ, используя: знания о КС и умение 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 КС,

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 КС.

Для блокирования несанкционированного исследования и копирования информации КС 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 брандмауэрами или файрволами – от нем. Brandmauer, англ. firewall – «противо-

пожарная 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.

Виды межсетевых экранов:

Бесплатные	Ashampoo FireWall Free * Comodo * Core Force (англ.) * Online Armor * PC Tools * PeerGuardian (англ.) * Sygate (англ.)
Проприетарные	Ashampoo FireWall Pro * AVG Internet Security * CA Personal Firewall * Jetico (англ.) * Kaspersky * Microsoft ISA Server * Norton * Outpost * Trend Micro (англ.) * Windows Firewall * Sunbelt (англ.) * WinRoute (англ.) * ZoneAlarm
Аппаратные	Fortinet * Cisco * Juniper * Check Point
FreeBSD	Ipfw * IPFilter * PF
Mac OS	NetBarrier X4 (англ.)
Linux	Netfilter (Iptables * Firestarter * Iplist * N * Shorewall) * Uncomplicated Firewall

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 приложе-

ния (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 нескольких 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 сводятся 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.

§ 3. Цифровая подпись

Первый в мире закон об электронной цифровой подписи был принят в марте 1995 г. Законодательным собранием штата Юта (США) и утвержден Губернатором штата. Закон получил название Utah Digital Signature Act. Ближайшими последователями штата Юта стали штаты Калифорния, Флорида, Вашингтон, где вскоре тоже были приняты соответствующие законодательные акты.

В качестве основных целей первого закона об электронной подписи были провозглашены: минимизация ущерба от событий незаконного использования и подделки электронной цифровой подписи; обеспечение правовой базы для деятельности систем и органов сертификации и верификации документов, имеющих электронную природу; правовая поддержка электронной коммерции (коммерческих операций, совершаемых с использованием средств вычислительной техники); придание правового характера некоторым техническим стандартам, ранее введенным Международным союзом связи (ITU – International Telecommunication Union) и Национальным институтом стандартизации США (ANSI – American National Standards Institute), а также рекомендациям Наблюдательного совета Интернета (IAB – Internet Activity Board), выраженным в документах RFC 1421 – RFC 1424.

Закон состоит из пяти частей. В первой части вводятся основные понятия и определения, связанные с использованием ЭЦП и функционированием средств ЭЦП. Здесь же рассматриваются формальные требования к содержательной части электронного сертификата, удостоверяющего принадлежность открытого ключа юридическому или физическому лицу.

Вторая часть закона посвящена лицензированию и правовому регулированию деятельности центров сертификации. Прежде всего, здесь оговорены условия, которым должны удовлетворять физические и юридические лица для получения соответствующей лицензии, порядок ее получения, ограничения лицензии и условия ее отзыва. Важным моментом данного раздела являются условия признания действительности сертификатов, выданных нелицензированными удостоверителями, если участники электронной сделки выразили им совместное доверие и отразили его в своем договоре. Фактически здесь закрепляется правовой режим сетевой модели сертификации, рассмотренной нами выше.

В третьей части закона сформулированы обязанности центров сертификации и владельцев ключей. В частности, здесь рассмотрены: порядок выдачи сертификата; порядок предъявления сертификата и открытого ключа; условия хранения закрытого ключа; действия владельца сертификата при компрометации закрытого ключа; порядок отзыва сертификата; срок действия сертификата; условия освобождения центра сертификации от ответственности за неправомерное использование сертификата и средств ЭЦП; порядок создания и использования страховых фондов, предназначенных для компенсации ущерба третьим лицам, возникшего в результате неправомочного применения ЭЦП.

Четвертая часть закона посвящена непосредственно цифровой подписи. Ее основное положение заключается в том, что документ, подписанный цифровой подписью, имеет ту же силу, что и обычный документ, подписанный рукописной подписью.

В пятой части закона рассмотрены вопросы взаимодействия центров сертификации с административными органами власти, а также порядок функционирования так называемых репозитариев – электронных баз данных, в которых хранятся сведения об изданных и отозванных сертификатах.

В целом закон об ЭЦП штата Юта отличается от других аналогичных правовых актов высокой подробностью.

Германский закон об электронной подписи (Signaturgesetz) был введен в действие в 1997 г. и стал первым европейским законодательным актом такого рода. Целью закона объявлено создание общих условий для такого применения электронной подписи, при котором ее подделка или фальсификация подписанных данных могут быть надежно установлены.

В этом Законе прослеживаются следующие основные направления: установление четких понятий и определений; подробное ре-

гулирование процедуры лицензирования органов сертификации и процедуры сертификации открытых ключей пользователей средств ЭЦП (правовой статус, порядок функционирования центров сертификации, их взаимодействие с государственными органами и другими центрами сертификации, требования к сертификату открытого ключа электронной подписи); рассмотрение вопросов защищенности цифровой подписи и данных, подписанных с ее помощью, от фальсификации; порядок признания действительности сертификатов открытых ключей.

Сейчас в США уже есть федеральный акт по ЭЦП. Его полное название – Electronic Signatures in Global and national Commerce Act – показывает, что основное назначение этого закона состоит в обеспечении правового режима цифровой электронной подписи в электронной коммерции.

Подписание этого Закона Президентом США состоялось в день национального праздника – 4 июля 2000 г. (День независимости), что должно придать этому законодательному акту особое значение. По мнению обозревателей, принятие данного закона символизирует вступление человечества в новую эру – эру электронной коммерции.

По содержанию сам этот Закон отличается краткостью. Он вводит ограниченное число основных понятий, устанавливает правовой режим электронной подписи и определяет компетенцию государственных органов, ответственных за функционирование ее инфраструктуры. Не сосредоточиваясь на конкретных правах и обязанностях центров сертификации, которым уделяется особое внимание в законодательствах других стран, Федеральный Закон США относит их к понятию инфраструктура ЭЦП и в самых общих чертах оговаривает взаимодействие элементов этой структуры с правительственными органами.

Если по своему основному смыслу германский Закон об электронной подписи является скорее регулирующим документом, то в США, в отличие от этого закона Германии, Федеральный Закон об электронной подписи США является координирующим правовым актом. Это связано с тем, что ко времени его принятия соответствующее регулирующее законодательство уже сложилось в большинстве отдельных штатов.

Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс представления компьютерной системе, который включает две стадии: идентификацию – пользователь сообщает системе по ее запросу свое имя (идентификатор); аутентификацию – пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль).

Для проведения процедур идентификации и аутентификации пользователя необходимы: наличие соответствующего субъекта (модуля) аутентификации; наличие аутентифицирующего объекта, хранящего уникальную информацию для аутентификации пользователя.

При этом различают две формы представления объектов, аутентифицирующих пользователя: внешний аутентифицирующий объект, не принадлежащий системе; внутренний объект, принадлежащий системе, в который переносится информация из внешнего объекта.

Внешние объекты могут быть технически реализованы на различных носителях информации – магнитных дисках, пластиковых картах и т.п. Естественно, что внешняя и внутренняя формы представления аутентифицирующего объекта должны быть семантически тождественны.

Рассмотрим теперь понятие электронной цифровой подписи (ЭЦП), зачем она нужна и как она применяется.

ЭЦП с некоторого времени является инструментом, благодаря которому упрощается движение документации. Причем происходит это не только внутри компании, но и за ее пределами.

Известно, что любой документ подписывает лицо, у которого есть такие полномочия. Делается это для того, чтобы придать документу юридическую силу. Благодаря современным технологиям, весь документооборот переходит в электронный вид.

Что же такое ЭЦП?

ЭЦП – это аналогия обычной подписи, которую применяют, чтобы придать юридическую силу документации, находящейся на электронном носителе. Хранят ее обычно на флэш-накопителе.

Сегодня в мире, полном электронных документов, подписание файла с помощью графических символов теряет смысл, так как подделать и скопировать графический символ можно бесконечное количество раз. Поэтому именно ЭЦП, являющаяся полным электронным аналогом обычной подписи на бумаге, но реализуемая не с помощью графических изображений, а с помощью математических преобразований над содержимым документа, полностью решает эту проблему.

При этом особенности математического алгоритма создания и проверки ЭЦП гарантируют невозможность подделки такой подписи посторонними лицами, чем достигается неопровержимость авторства.

ЭЦП выступает как **реквизит электронного документа**, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца ключа, а также установить отсутствие искажения информации в электронном документе.

Сама по себе ЭЦП представляет собой определенную последовательность символов, которая формируется в результате преобразования исходного документа (или любой другой информации) при помощи специального программного обеспечения. ЭЦП добавляется к исходному документу при пересылке. ЭЦП является уникальной для каждого документа и не может быть перенесена на другой документ. Невозможность подделки ЭЦП обеспечивается значительным количеством математических вычислений, необходимых для её подбора. Таким образом, при получении документа, подписанного ЭЦП, получатель может быть уверен в авторстве и неизменности текста данного документа.

Пользоваться электронной подписью достаточно просто. Никаких специальных знаний, навыков и умений для этого не потребуется. Каждому пользователю ЭЦП, участвующему в обмене электронными документами, генерируются уникальные открытый и закрытый (секретный) криптографические ключи.

Закрытый ключ – это закрытый уникальный набор информации объемом 256 бит, хранится в недоступном другим лицам месте на дискете, смарт-карте, ru-token. Работает закрытый ключ только в паре с открытым ключом.

Открытый ключ – используется для проверки ЭЦП получаемых документов/файлов. Технически это набор информации объемом 1024 бита.

Открытый ключ передается вместе с вашим письмом, подписанным ЭЦП. Дубликат открытого ключа направляется в Удостоверяющий центр, где создана библиотека открытых ключей ЭЦП. В библиотеке Удостоверяющего центра обеспечивается регистрация и надежное хранение открытых ключей во избежание попыток подделки или внесения искажений.

Вы устанавливаете под электронным документом свою электронную цифровую подпись. При этом на основе секретного закрытого ключа ЭЦП и содержимого документа путем криптографического преобразования вырабатывается некоторое большое число, которое и является электронно-цифровой подписью данного пользователя под данным конкретным документом. Это число добавляется в конец электронного документа или сохраняется в отдельном файле.

В подпись в том числе записывается следующая информация**:** имя файла открытого ключа подписи, информация о лице, сформировавшем подпись, дата формирования подписи.

Пользователь, получивший подписанный документ и имеющий открытый ключ ЭЦП отправителя, на основании текста документа и открытого ключа отправителя выполняет обратное криптографическое преобразование, обеспечивающее проверку электронной цифровой подписи отправителя. Если ЭЦП под документом верна, то это значит, что документ действительно подписан отправителем и в текст документа не внесено никаких изменений. В противном случае будет выдаваться сообщение, что сертификат отправителя не является действительным.

Приведем теперь основные термины и определения, относящиеся к процедуре получения и пользования ЭЦП.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц,

определенный ее владельцем или соглашением участников этой информационной системы.

Удостоверяющий центр – юридическое лицо, выполняющее функции по: изготовлению сертификатов ключей подписей, созданию ключей электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи, приостановлению и возобновлению действие сертификатов ключей подписей, а также аннулированию их, ведению реестра сертификатов ключей подписей, обеспечению его актуальности и возможности свободного доступа к нему участников информационных систем, проверке уникальности открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра, выдаче сертификатов ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии, осуществлению по обращениям пользователей сертификатов ключей подписей подтверждения подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей, предоставлению участникам информационных систем иных связанных с использованием электронных цифровых подписей услуг.

При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Подчеркнем, что правовое обеспечение электронной цифровой подписи следует понимать не только как совокупность нормативно-правовых актов, обеспечивающих правовой режим ЭЦП и средств ЭЦП. Это гораздо более широкое понятие. Оно лишь начинается с

государственного закона об электронной цифровой подписи, но развивается далее и впоследствии охватывает все теоретические и практические вопросы, связанные с электронной коммерцией вообще.

Таким образом, основные преимущества ЭЦП следующие: упрощает и ускоряет процесс обмена данными (когда ведется сотрудничество с зарубежными компаниями); сокращение расходов, связанных с документооборотом; повышение уровня безопасности для информации, носящей коммерческий характер.

С понятием ЭЦП тесно связаны два других: **ключ и сертификат электронной подписи**. Сертификат подтверждает, что ЭП принадлежит конкретному лицу. Он бывает усиленным и обычным. Усиленный сертификат выдается либо удостоверяющим центром, либо ФСБ.

Ключ – это символы, находящиеся в последовательности. Обычно они используются парой. Первый – это сама подпись, другой подтверждает, что она подлинная. Для подписи каждого вновь создаваемого документа формируется новый ключ.

Впервые ЭЦП стали использоваться в России в 1994 году. А закон о регулировании их применения был принят в 2002. Он был крайне расплывчатым и неоднозначно толковал терминологию. Вопрос получения подписи также в нем практически не освещался. Затем, начиная с 2011 года на электронный документооборот перешли государственные структуры, а все должностные лица получили ЭЦП. И в 2012 году этот процесс приобрел глобальные масштабы, и, благодаря этому, мы сейчас можем стать обладателями универсальных современных подписей.

Как получить личную электронную цифровую подпись?

Чтобы получить электронную цифровую подпись, нужно прой-

ти несколько важных ступеней: определиться с видом подписи; выбрать удостоверяющий центр; заполнить заявку; оплатить выставленный счет; собрать необходимый пакет документации; получить ЭЦП.

Для получения ЭЦП физические лица должны собрать следующий набор документации: заполненный бланк заявления; паспорт с ксерокопией; ИНН; СНИЛС; квитанция, подтверждающая оплату счета.

Если у получателя есть доверенное лицо, подачей документов может заняться оно. Однако нужна доверенность на совершение таких действий.

Практическое задание

1. Шаг первый – выбор вида подписи.

За последний период времени увеличилось количество тех, кто хочет получить **усиленную электронную подпись**. Это объясняется тем, что она может подтвердить не только личность отправившего документ, но и является защищенной по максимуму. По мнению ряда экспертов, простые ЭЦП в скором времени прекратят свое существование.

2. Шаг 2 – выбор удостоверяющего центра (УЦ). Если ЭЦП нужно получить, чтобы сдавать отчеты, выбирайте квалифицированную, если же просто вести документооборот, то простую. Уточним, что УЦ является юрлицом, цель работы которого – формирование и выдача ЭЦП.

Кроме этого, УЦ осуществляет следующую деятельность:

– подтверждает, что подпись достоверна;

– при необходимости блокирует ЭЦП;

– является посредником, если вдруг возникает конфликтная ситуация;

– оказывает техническую поддержку; предоставляет необходимое ПО клиентам.

В РФ сегодня насчитывается около 100 УЦ. Лучше выбрать тот,

который подходит по вашему месторасположению и возможностям. Сделать это просто: достаточно просмотреть информацию на официальном сайте.

3. Шаг 3 – оформление заявки. Для этого необходимо либо посещение офис УЦ, либо заполнить ее в режиме онлайн. Удаленный способ позволяет избежать личного посещения УЦ, то есть сэкономить некоторое количество времени.

Как только отправка заявки будет завершена, с клиентом связывается специалист УЦ, чтобы уточнить указанные в ней данные. Ему можно задать вопросы и получить консультацию.

4. Шаг 4 – оплата ЭЦП. Оплатить услугу необходимо заранее. Как только заявка будет принята, все детали согласованы, клиенту выставляется счет. Стоимость может варьироваться, так как она зависит от региона, где проживает клиент, от самой компании и от того, какую ЭЦП вы хотите получить. Причем разброс цен довольно большой – от 1500 до 8000 рублей.

5. Шаг 5 – сбор документов для ЭЦП. При сборе документов важным нюансом является следующий: ЭЦП нужна для физического лица, ЭЦП для юридического лица либо для ИП. Поэтому характеризовать документацию будем по отдельности.

Юридические лица должны подготовить:

– заполненное заявление;

– свидетельство ОГРН;

– свидетельство ИНН; выписку из ЕГРЮЛ (не просроченную);

– паспорт с копией того лица, которое будет использовать ЭЦП;

– квитанцию об оплате;

– СНИЛС лица, которое будет использовать ЭЦП;

– если подпись будет использовать директор, нужно предоста-

вить приказ, на основании которого он занимает эту должность;

– для других сотрудников нужны доверенности, чтобы они могли использовать ЭЦП.

Индивидуальные предприниматели:

– заполненное заявление;

– свидетельствово ОГРНИП;

– свидетельство ИНН; выписку из реестра предпринимателей, которой не более 6 месяцев (можно копию);

– квитанцию, которая подтвердит оплату.

Если заявка была подана удаленно, нужные документы направляют в УЦ по почте, если лично – то вместе с заявкой. При этом для физических лиц есть два типа подписей: квалифицированная и неквалифицированная. Процедура получения, если сравнивать с юридическими лицами, гораздо проще. Частные лица обычно используют ЭЦП, чтобы подписывать бумаги.

Сейчас для ее применения разработаны такие системы для получения различных сведений: Единый портал государственных услуг; сеть ЕСИА. Для ЕСИА достаточно простого типа ЭП, а вот для портала государственных услуг используется квалифицированная.

Чтобы получить ЭЦП, гражданин также обращается в УЦ, со всеми документами и заявлением. Также при себе нужно иметь флэш-накопитель, на который запишут закрытую часть ключа, известную только владельцу.

Обычная процедура выглядит так: обратиться в УЦ за сертификатом и получением ключа ЭЦП; подобрать пароль; заполнить бланки для получения ключей; подать все документы; получить сертификат на ключи.

Порядок получения ЭЦП юридическим лицом практически не отличается от получения подписи физическим лицом. Точно так же выбирается УЦ, собираются все нужные документы, оплачивается выставленный счет. Сам процесс подготовки ЭЦП занимает около 5 дней.

Теперь о хеш-функции – зачем она нужна?

Хеш-функция является уникальным числом, которое получают из документа, преобразовав его с помощью алгоритма. Она обладает повышенной чувствительностью к разного рода искажениям документа: если изменится хотя бы один знак в первоначальном документе, исказится большая часть знаков хеш-значения.

Хеш-функция устроена так, что по ее значению исходный документ восстановить невозможно, также нельзя найти два разных электронных документа, у которых одно и то же хеш-значение.

При формировании ЭЦП отправитель вычисляет хеш-функцию документа и шифрует ее при помощи секретного ключа. Затем она будет нужна для упрощения обмена данными между пользователями. Это ключевой инструмент по защите данных. После всего этого подписываемый файл проходит процедуру хеширования. А получатель сможет удостовериться в подлинности документа.

Юридическая сила ЭЦП. ЭЦП обладает равной юридической силой с обычной подписью в бумажном варианте документа, в том случае если она наносилась без нарушений. Если же были выявлены отклонения, документ силы не имеет. Государство регулирует процесс использования ЭЦП федеральным законодательством.

ЭЦП действительна в течение 12 месяцев, с того дня, когда она была получена**.** Как только этот срок заканчивается, ее продлевают либо получают другую.

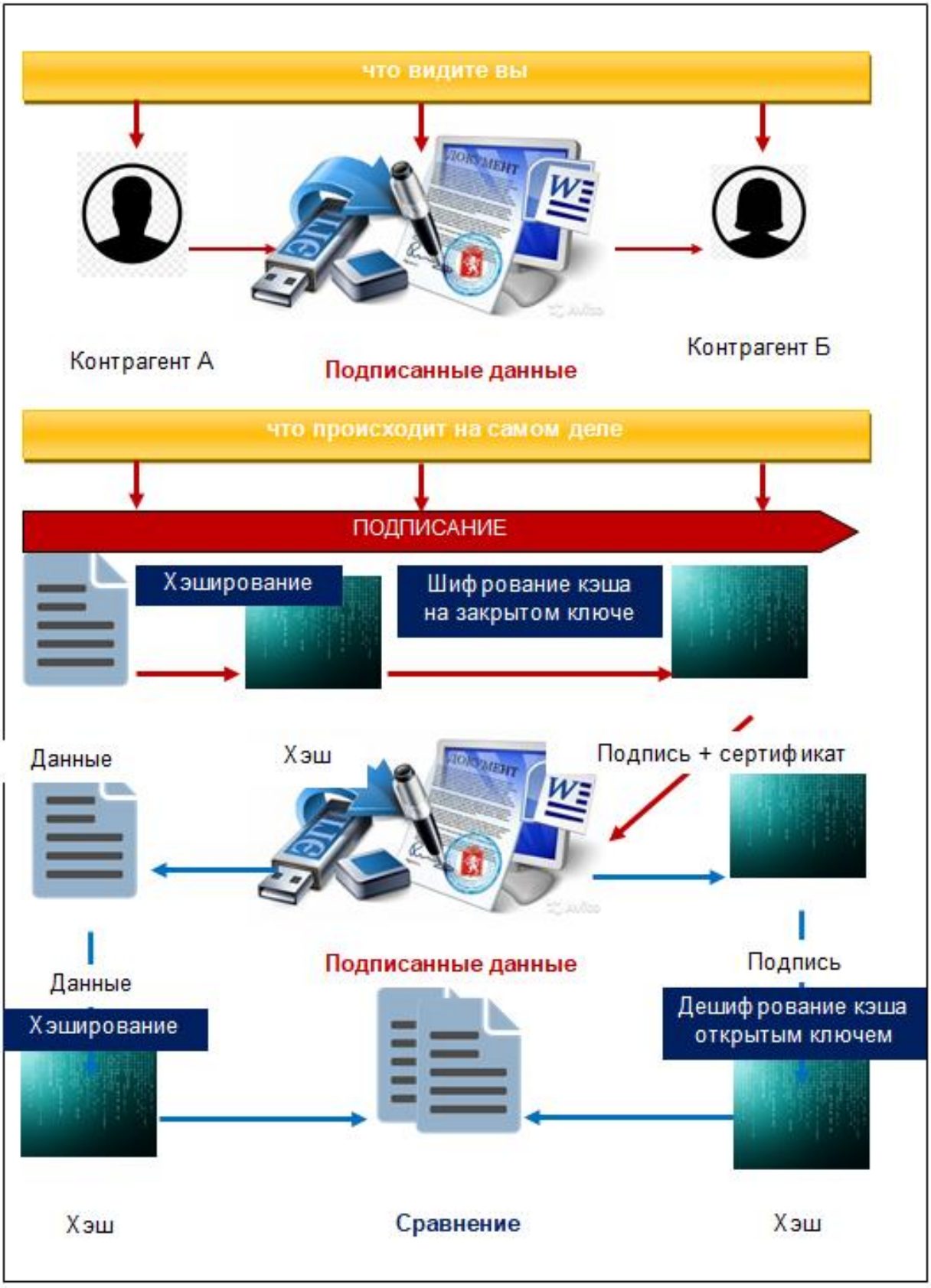

Рис. 28. Схема функционирования ЭЦП

Где особенно важно и необходимо использование ЭЦП? Выделим основные сферы применения ЭЦП.

Электронный документооборот. Технология ЭП широко используется в системах электронного документооборота различного назначения: внешнего и внутреннего обмена, организационно-распорядительного, кадрового, законотворческого, торгово-промышленного и прочего. Это продиктовано главным свойством электронной подписи – она может быть использована в качестве аналога собственноручной подписи и/или печати на бумажном документе.

Во внутреннем документообороте ЭП используется как средство визирования и утверждения электронных документов в рамках внутренних процессов. Например, во время согласования договора директор подписывает его ЭП, что значит, что договор утвержден и может быть передан в исполнение.

При построении межкорпоративного документооборота (B2B) наличие ЭП является критически важным условием обмена, поскольку является гарантом юридической силы. Только в этом случае электронный документ может быть признан подлинным и использоваться в качестве доказательства в судебных разбирательствах. Подписанный усиленной электронной подписью документ также может длительное время храниться в цифровом архиве, сохраняя при этом свою легитимность.

Электронная отчетность для контролирующих органов. Многие компании наверняка уже оценили удобство сдачи отчетности в электронном виде. Современный подход к сдаче отчетности через интернет состоит в том, что клиент может выбрать любой удобный для себя способ: отдельное ПО, продукты семейства 1С, порталы ФНС, ФСС. Основа этой услуги – сертификат электронной подписи, который должен быть выпущен надежным удостоверяющим

центром, метод же отправки не имеет решающего значения. Такая подпись нужна для придания документам юридической значимости.

Государственные услуги. Каждый гражданин Российской Федерации может получить электронную подпись для получения госуслуг. С помощью ЭП гражданин может заверять документы и заявления, отправляемые в ведомства в электронном виде, а также получать подписанные письма и уведомления о том, что обращение принято на рассмотрение от соответствующих органов власти.

Пользователь имеет возможность подписать электронной подписью заявление, отправляемое в орган исполнительной власти (при готовности органа исполнительной власти принимать заявления, подписанные электронной подписью).

При реализации этого механизма используются отечественные стандарты ЭП (ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001) и применяются сертифицированные в системе сертификации ФСБ России средства криптографической защиты информации, такие как «Aladdin e-Token ГОСТ» и «КриптоПро CSP», что дает основания считать данную подпись усиленной квалифицированной электронной подписью (Источник: портал Госуслуги).

Электронные торги. Электронные торги проходят на специальных площадках (сайтах). Электронная подпись необходима поставщикам на государственных и коммерческих площадках. ЭП поставщиков и заказчиков гарантируют участникам, что они имеют дело с реальными предложениями. Кроме того, заключенные контракты приобретают юридическую силу только при его подписании обеими сторонами.

Арбитражный суд. При возникновении каких-либо споров между организациями в качестве доказательства в суде могут использоваться электронные документы. Согласно Арбитражному процессуальному кодексу РФ, полученные посредством факсимиль-

ной, электронной или иной связи, подписанные электронной подписью или другим аналогом собственноручной подписи, относятся к письменным доказательствам. Об этом подробнее ниже.

Документооборот с физическими лицами. Надо признать, данная сфера применения ЭП весьма специфична и пока редко используема, тем не менее возможна. С помощью ЭП заверять различные документы могут физические лица. Благодаря этой возможности удаленные работники на основании договоров оказания услуг, например, могут выставлять акты приемки-сдачи работ в электронном виде.

Таким образом, мы видим, что использование ЭЦП наибольшую выгоду приносит крупным компаниям и предприятиям. Благодаря ей удешевляется документооборот, открываются широкие горизонты для бизнеса. Простым гражданам иметь ЭЦП также полезно – например, заказывать госуслуги с ЭЦП можно не выходя из дома.

§ 4. Правовая защита информации и интеллектуальной собственности в цифровой экономике

С развитием цифровой экономики все более важную роль начинает играть формирование эффективной системы управления интеллектуальной собственностью (ИС). Это подразумевает, прежде всего, создание современных методов ее защиты и механизмов коммерциализации. Россия сегодня находится в начале процесса создания такой системы, которая позволит сформировать полноценный рынок интеллектуальной собственности и адаптировать законодательство к вызовам цифровой экономики.

Цифровая экономика характеризуется постоянным увеличением потоков информации, идей и инноваций. Происходит мгновенный обмен виртуальными товарами: электронными книгами, прило-

жениями, онлайн-играми, музыкальными файлами и др. Растет число публичных интернет-платформ – социальные сети, мессенджеры, медиа-площадки, магазины и пр. С развитием электронной коммерции возрастает быстрота появления новых торговых марок и других объектов интеллектуальной собственности.

При этом сам процесс формирования глобальной регулирующей и контролирующей ИС-системы еще далек от полного завершения. Но ряд механизмов уже создан. Среди них – следующие.

Правовое регулирование. В настоящий момент действует Сингапурский договор о законах по товарным знакам, гармонизирующий регулирование их регистрации в разных странах, в том числе с учетом информационно-коммуникационных технологий.

В ряде стран интернет-провайдеры обязаны уведомлять подписчиков, когда их учетная запись используется для распространения нарушающего закон контента, и предупреждать их о последствиях.

Кроме того, для защиты активов от неправомерного использования и хищения в условиях глобального информационного обмена в 2016 году усовершенствовано законодательство о коммерческой тайне: в ЕС – директива Trade Secrets Directive, в США – закон об охране коммерческой тайны. Растет число стран, учреждающих специализированные суды и другие инстанции для разрешения споров по интеллектуальной собственности.

Глобальные инструменты проверки информации, позволяющие предотвратить нарушение прав ИС. Система поиска зарегистрированных торговых марок через интернет TMclass и база данных по брендам Всемирной организации интеллектуальной собственности (ВОИС). Компании, которые занимаются подтверждением авторства с помощью блокчейн: Ascribe, Bitproof, Blockai, Stampery и др.

При этом в условиях цифровой экономики интеллектуальная собственность становится ключевым инструментом извлечения прибыли. Появляются все новые способы для маркетингового и информационного продвижения объектов ИС.

Например, новые возможности дает использование новых доменов верхнего уровня, порядок предоставления которых заметно упростился. Но пока бизнес не готов в полной мере использовать эти преимущества. По данным корпорации ICANN, из-за недостаточной поддержки новых доменов теряется 3,6 млрд, а из-за недостаточной поддержки IDN (доменов, в названии которых используются национальный алфавит) – $6,2 млрд.

При этом цифровая экономика – это не только блокчейн и криптовалюты, о которых так много говорят в последнее время, но и цифровые продукты – все, что поддается оцифровке или изначально производится в цифровой форме. Первым таким продуктом был сигнал, передаваемый в цифровой форме по каналам связи без искажений (бит в бит). А сейчас на алгоритмах и криптографии основаны «умные контракты», а также активно обсуждаемые в последнее время идеи об управлении правами интеллектуальной собственности на основе блокчейн.

Самым известным и самым обсуждаемым проектом здесь, безусловно, является проект IPCHAIN. Впервые идея такого проекта была озвучена в конце 2016 года, а потом обсуждалась на различных форумах, неизменно вызывая большой интерес. Начнем с рассмотрения такого интеллектуального продукта, как авторские и смежные права.

Действительно, легкость копирования оцифрованных произведений постоянно растет по мере совершенствования технических средств. Авторское право всегда отвечало на это ужесточением норм. Самый яркий пример – Digital Millennium Copyright Act, где

появилось сразу несколько немыслимых ранее для авторского права запретов, в том числе на ввоз в США некоторых технических средств. Говорящее название этого закона прямо связывает его с цифровой эпохой и, разумеется, с цифровой экономикой.

Но если в 90-е годы, когда принимался этот закон, речь шла в основном о копировании на диски, то сегодня это уже не актуально. Главное – передача через интернет клонов цифрового продукта – та самая передача сигнала (бит в бит), о которой говорилось выше. В этих условиях бороться с несанкционированным копированием и распространением цифрового контента становится сложно и дорого. Среди предлагаемых решений можно найти: запрет наиболее эффективных технологий копирования и распространения цифровых продуктов; «Глобальную лицензию», т.е. разрешение беспрепятственного распространения цифрового контента в интернете и обложения сбором всего бизнеса, извлекающего из этого выгоду, включая не только продавцов гаджетов, но и провайдеров; использование технологии блокчейн, когда продукты распространяются свободно, но в зашифрованном виде, а ключ получает только легальный покупатель.

Каждое из этих предложений имеет свой набор недостатков. Запрет наиболее эффективных технологий – тот же луддизм, его история показывает, что стоять на пути технического прогресса контрпродуктивно. Однако российский законодатель пока уверенно движется именно по этому пути. «Глобальная лицензия» тянет за собой шлейф злоупотреблений, так как собранные деньги надо как-то распределять. А как?

Наконец, третий путь – шифрование и ключи в первом приближении очень похожи на разрешение скачать продукт только после оплаты. Разница, разумеется, есть. Блокчейн – не только шифрование и ключи, но и возможность узнать, кто именно допустил «утечку» продукта. В некотором смысле продукты перестают быть клонами, каждому клону можно добавить индивидуальную метку.

Но как только появится технология, позволяющая эту метку стирать, все вернется на круги своя. И все же луч надежды здесь есть, есть, что обсуждать.

Вторая проблема, предположительно решаемая с помощью блокчейн, связана с коллективным управлением авторскими и смежными правами. Здесь тоже упор делается на прозрачность трансакций. Но это касается только тех авторов или иных правообладателей, кто поручил управление своими правами обществу (ОКУП) соответствующего профиля. А как быть с правами тех, кто никому управлять ими не поручал? Из блокчейн для членов ОКУП они выпадают. Следовательно, аккредитованные ОКУП продолжат собирать лицензионные платежи за них. А как? Вопросов много, а ответов пока мало, если они вообще есть.

Возможно, надо резко сократить номенклатуру охраняемого контента, реально обеспечивая защиту только зарегистрированным произведениям, когда авторы явно выразили свою позицию.

Теперь – о проблеме защиты **промышленной собственности**. Ограничимся здесь только патентами и ноу-хау, причем патентами только на изобретения и только такими ноу-хау, которые можно полностью описать, а потом зашифровать и передать по каналам связи. Спрашивается, что здесь можно улучшить с помощью технологии блокчейн?

Во-первых, патентные системы всех стран подчиняются ряду общих для всех правил, закрепленных в международных конвенциях, прежде всего, в Парижской конвенции.

Во-вторых, есть уже накопленный массив запатентованных изобретений. Менять можно некоторые детали, но не принципы работы патентной системы, а лучше вообще ничего в ней не менять, а вписываться в существующие нормы. Они не без причин появились, а в результате огромной работы большой массы опытных в этом деле людей.

А теперь вопрос: что предлагается передавать на основе умного контракта? Если описание изобретения, то теряется суть патента – раскрытие формулы изобретения в обмен на легальную монополию. А если не описание изобретения, тогда что? Ответ у инициаторов IPCHAIN, возможно, есть. Но его хотелось бы услышать.

С передачей ноу-хау, на первый взгляд, дело обстоит лучше. Информация, составляющая суть ноу-хау, шифруется, добросовестному покупателю выдается ключ. Но не все так просто. Покупатель (лицензиат) должен быть уверен в работоспособности приобретаемого ноу-хау. Если там все зашифровано, как эту уверенность можно обеспечить, не расшифровывая содержание?

Кроме того, существует «золотое правило патентования» – устройство патентуй, технологию охраняй как ноу-хау. Устройство рано или поздно попадет в руки конкурента, он поймет, как оно устроено, а это – добросовестное получение сведений, составляющих ноу-хау. Значит, надо патентовать. Зато технологию можно использовать, не допуская посторонних наблюдателей. Получается, что и в том и другом случае блокчейн как-то не встраивается.

И еще одна проблема – неизбежность комбинаторного взрыва при масштабировании блокчейн. Комбинаторный взрыв лучше всего характеризуют шахматы. Интуиция здесь жестоко обманывает человека. А потому нельзя думать, что мощные компьютеры решат все проблемы. Предел ближе, чем кажется.

Даже относительно простые контракты при продаже компьютерных игр предусматривают несколько случаев, когда решение надо принимать не заранее, а исходя из конкретных обстоятельств. Это создает все условия для комбинаторного взрыва и большие проблемы для «умных» контрактов. Очень может быть, что и тут возможности технологии блокчейн сильно преувеличены. Недооценивать их тоже было бы ошибкой. Надо изучать и обсуждать.

Рассмотрим также проблему так называемого **«пиратства»**. «Пиратство – это, безусловно, самая большая головная боль всего рынка легального аудио- и видеорынка в интернете, потому что, при всем рабочем механизме действующего пиратского законодательства, количество еще не перешло в качество. При более чем 120 заблокированных сайтов относительно общего числа пиратских сайтов это ничтожная доля, которая никак не повлияла на общую картину. «Сама механика отработана хорошо, но чтобы масштаб блокировок перерос в существенное снижение пиратского контента – до этого далеко», – подчеркнул гендиректор Ассоциации «Интернет-видео» Алексей Бырдин.

Как отметила генеральный директор онлайн-кинотеатра Tvzavr Марина Сурыгина, необходимо как можно быстрее рассмотреть законопроект о зеркальных сайтах, который в настоящее время находится в Госдуме. Проектом предусматривается два очень важных для отрасли изменения: во-первых, он позволит блокировать зеркальные сайты в ускоренном порядке, а во-вторых, позволит удалить их из поисковой выдачи. «Это очень важная норма, потому что для подавляющего большинства пиратских сайтов основным источникам трафика является поисковая система. Зачистка поисковой выдачи – это один из важнейших инструментов, которые в мировой практике доказали свою эффективность, потому что Google, например, уже давным-давно обязан даже без судебного решения, а по требованию правообладателя удалять ссылки на пиратский контент», – пояснил Бырдин.

Как уточнила Сурыгина, важными вопросами в этой сфере являются экономическая поддержка отрасли интернет-кинотеатров со стороны государства, например, признанием их IT-компаниями с соответствующими льготами по налогообложению, а также дальнейшее сокращение цифровых окон, то есть времени между окончанием кинотеатрального проката фильма и его выхода на онлайн-носителях.

«Мы провели исследование, которое показало, что пик пиратских скачиваний приходится на этот промежуток между тем, когда фильм перестали показывать в кинотеатре, но его еще нельзя посмотреть легально. Как только картину можно посмотреть, например, по smart tv, люди перестают ее скачивать нелегально», – отметил Бырдин. Также Сурыгина добавила, что необходимо решить проблемы с выдачей прокатных удостоверений для показа фильма в интернете. «Они не нужны, во многих случаях, просто вредны, так как приведут к расцвету пиратства», – заметила собеседница агентства.

В то же время Бырдин подчеркнул, что, несмотря на необходимость борьбы с пиратством, успех различных легальных платформ распространения видео- и аудиоконтента напрямую от этого не зависит. «Мы видим, где происходит рост, – он происходит на платформах smart tv и на мобильных устройствах. Это закрытые экосистемы, в которых нельзя установить пиратское приложение, потому что там происходит ручная модерация и фильтрация подобного рода приложений. Поэтому в этих онлайн-кинотеатрах существует искусственно зачищенная легальная среда. И наши граждане, которые, как все привыкли думать, не готовы платить за контент, прекрасно платят за качественный контент в красивом интерфейсе, сидя у себя на диване. Никакого барьера психологического и экономического у людей нет вообще», – рассказал эксперт.

Как считает гендиректор АО «Фирма Мелодия» Андрей Кричевский, необходимо создать эффективный механизм защиты авторских и смежных прав в интернете. При этом надо четко понимать, что такой механизм именно в интернете никогда не будет эффективным, если он будет существовать исключительно как формальный инструмент. Реальные же инструменты защиты интересов правообладателей должны носить экономический, а не запретительный характер – в первую очередь надо обеспечить достойное вознагражде-

ние обладателям авторских и смежных прав за использование их собственности интернет-пользователями. «Только в этом случае мы сможем обоснованно требовать обеспечить доступность и открытость объектов музыкальной культуры. При ином подходе такие требования станут носить экспроприационный или даже грабительский характер», – подчеркнул собеседник агентства.

При этом, по словам Бырдина, важно не только платить деньги авторам, но и создать механизм, при котором пиратам будет невыгодно заниматься этим бизнесом. «Нужно четко давать себе отчет в том, что это бизнес на результатах чужого труда. Деньги там зарабатываются на рекламе, в том числе запрещенного в России бизнеса. Поэтому нужно поднять вопрос с рекламным регулятором в лице ФАС, потому что то прямое нарушение, и с Роскомнадзором, который технически является основным ведомством по борьбе с незаконной рекламой. На стыке между этими двумя ведомствами лежит решение этой проблемы».

В конце 2010 – начале 2011 года группа видных британских экспертов под руководством профессора И. Харгривса (Ian Hargreaves) по поручению премьер-министра Дэвида Кэмерона провела изучение текущего состояния законодательства Великобритании об интеллектуальной собственности. Премьер-министр подчеркнул важность данного исследования, выразив опасение, что недостатки правовой системы могут препятствовать инновациям и развитию экономики. В мае 2011 года был подготовлен подробный отчет «Цифровые перспективы: Независимый обзор интеллектуальной собственности и развития».

На основной вопрос, поставленный перед учеными, был дан утвердительный ответ – да, действительно, действующее британское законодательство негативно влияет на экономический рост и сдерживает инновации. Заключение содержит детальный обзор основных проблем в различных сферах интеллектуальной собственности и

10 рекомендаций по их разрешению. Особенно много внимания уделено влиянию интернета и цифровых технологий на оборот творческих результатов. Я бы даже сказал, что эксперты целенаправленно развенчивают некоторые укоренившиеся в обществе мифы: о последствиях пиратства, способах борьбы с ними и так далее.

Данный отчет был признан одним из самых авторитетных в своей области. С тех пор на него часто ссылаются эксперты и правоприменители не только в Великобритании, но и во многих других странах Евросоюза. Представляется, что краткое рассмотрение его основных позиций будет для многих очень полезным.

Рекомендации ученых были сосредоточены вокруг 10 основных тем. Вначале в Докладе описывается все возрастающая роль результатов интеллектуальной деятельности в современной экономике – отмечая, что в 2008 году в Великобритании объем инвестиций в нематериальные активы превысил вложения в активы материальные (£137 миллиардов и £104 миллиарда соответственно).

В Докладе подчеркивается, что цифровые технологии, наиболее важные и постоянно изменяющиеся сегодняшние технологии, тесно связаны с экономическим ростом, развитием существующих и появлением новых рынков. А в самом их сердце находятся права на интеллектуальную собственность. Внедрение новых технологий, например, таких масштабных, как облачное программирование и «интернет вещей», напрямую зависит от состояния и возможностей системы интеллектуальных прав. Отсюда следует беспрецедентное влияние права интеллектуальной собственности не только на текущую экономическую ситуацию, но и ее будущие трансформации.

При этом авторы отмечают, что по многим моделям правового регулирования использования творческих результатов собрано крайне мало объективных данных. Государственная политика в отношении развития права интеллектуальной собственности должна

опираться на надежную базу проверенных и достоверных фактов.

При этом ярким примером непродуманности правового регулирования авторы называют принятую в Евросоюзе Директиву «О гармонизации и улучшении правовой охраны баз данных». Она была принята, чтобы стимулировать инвестиции в разработку баз данных, которые существенно отставали от объема инвестиций в ряде стран, в частности США (где, кстати, вообще не были закреплены права на базы данных). Последующие исследования показали, что после принятия Директивы количество созданных в ЕС баз данных серьезно снизилось, тогда как в США они по-прежнему разрабатывались все в большем объеме.

Что же касается международных приоритетов, то в основном здесь речь идет о достаточно понятных вещах: необходимости тесного сотрудничества Великобритании с Евросоюзом и другими странами и поддержания национальных интересов в сфере права интеллектуальной собственности в свете растущего влияния развивающихся рынков, поскольку Великобритания является достаточно крупным экспортером продукции, содержащей результаты интеллектуальной деятельности. В этой связи стоит всячески содействовать внедрению европейского патентного суда и единой патентной системы Евросоюза.

Эксперты также напоминают, что в последние двадцать лет бурное развитие всемирной сети неоднократно ставило под сомнение саму идею авторского права как охраняемого источника дохода авторов, поскольку она вступала в противоречие с неуправляемой и некоммерческой сущностью интернета.

И лишь в относительно недавнее время стали приживаться различные онлайновые бизнес-модели, внедряемые, прежде всего, крупными корпорациями, а затем и малыми и средними предприятиями (SME). Фирмы SME получили серьезные преимущества от ис-

пользования новых цифровых технологий, позволившие им активно внедрять инновации, увеличивать количество рабочих мест и приобретать свою нишу на национальных рынках. Около 5,6% ВВП Великобритании обеспечивают предприятия творческих отраслей экономики. Широко используемые ими авторско-правовые лицензии становятся стратегически важными для поддержания экономического роста.

При этом цифровые технологии первоначально крайне отрицательно влияли на такие сферы, как издание газет, журналов и книг, звукозапись, производство телепрограмм, кинофильмов и видеоигр и так далее. Предприниматели вынуждены были серьезно перестраивать свои методы ведения бизнеса в попытке сохранить прибыль. Далеко не всегда внедряемые ими схемы оказывались эффективными или достаточно простыми, чтобы клиенты и потребители готовы были их использовать.

Так, в Великобритании насчитывается порядка 70 музыкальных сервисов, предоставляющих легальный цифровой контент, что гораздо больше, чем в США. Сложность условий их работы до сих пор не позволяет им одерживать сколько-нибудь заметных побед в битве с бесплатными нелегальными сервисами. Весомая доля «сложности» приходится на особенности лицензирования: трудности поиска огромного количества правообладателей, необоснованный уровень платы, запутанные условия выдачи лицензий и тому подобные обстоятельства.

Помогут в такой ситуации, по мнению авторов, те же самые цифровые технологии, а именно: автоматическое лицензирование, или механическое управление правами и согласование условий использования между устройствами без участия человека.

Подобные разработки выгодны всем участникам по следующим причинам:

– авторы контента получат более легкий доступ на рынок, в том числе возможность выдавать лицензии и получать вознаграждение без участия посредников, снизится количество произведений-«сирот» (владельцев которых установить затруднительно), а условия предоставления лицензий будут более прозрачными;

– посредники в реализации интеллектуальных прав, располагая достаточной информацией об авторах и их агентах (в том числе иностранных), об условиях и содержании лицензий, будут поддерживать открытость и конкурентоспособность рынка, что приведет к снижению транзакционных издержек;

– потребители и иные пользователи получат больший выбор, лучший сервис и меньшие цены на использование интересующего их контента.

Эксперты признают, что сама их идея не нова. Призывы к созданию региональных или общемировых баз данных различных объектов интеллектуальной собственности, к разработке схем глобального лицензирования раздавались не раз.

Были даже отдельные попытки реализовать их на практике. В качестве примера приводятся такие проекты, как Accessible Registries of Rights Information and Orphan Works (Arrow), Automated Content Access Protocol (ACAP), Global Repertoire Database, Picture Licensing Universal System (Useplus), the ONIX standards for Books, Serials and Licensing Terms, OnLineArt (OLA). По разным причинам ни один из них так и не стал общепризнанным стандартом в сфере цифрового лицензирования.

Исследователи уверены, что рано или поздно какие-либо проекты будут реализованы в широком масштабе. Пока же государствам (и в особенности Великобритании) стоит взять на себя роль организаторов и координаторов процесса, что даст им серьезные экономические преимущества.

Негативный пример взаимодействия государства и участника цифрового рынка авторы отчета видит в истории с компанией Google и ее проектом по оцифровке книг. Google Books вполне мог бы стать первым шагом к созданию модели глобального онлайнового лицензирования. Но вместо обсуждения вариантов сотрудничества правообладатели добились в суде признания действий интернет-компании незаконными. Действия Google вызвали серьезные опасения у тех, кто увидел за ними недобросовестную попытку получить преимущества и ограничить конкуренцию. Активность и масштаб деятельности интернет-гиганта этому только способствовали. Но именно эти факторы, по мнению экспертов, должны стать отправной точкой в сдержанных, тщательных и не предвзятых переговорах, поскольку дают шанс действительно изменить международный рынок цифрового контента.

Схема цифрового лицензирования должна включать разработку технологических методов добавления к цифровому контенту сведений об авторах, их агентах, условиях предоставления лицензии и использования материалов (метаданные), создание онлайновых баз данных контента и возможностей автоматического обмена информацией и получения лицензий.

Схема должна быть технологически нейтральной, то есть допускать ее использование самыми различными сервисами, в том числе теми, которые могут появиться в будущем. Должна быть также внедрена система рассмотрения возникающих споров с минимальными издержками. Необходимо также достичь договоренности с интернет-поисковиками, чтобы они облегчали своим пользователям обнаружение легального контента.

Модель цифрового лицензирования предусматривает создание так называемой Цифровой Биржи авторских прав (Digital Copyright Exchange), структуры, обеспечивающей ведение онлайновых баз данных и дистанционное заключение лицензионных договоров.

Авторы Доклада также отмечают, что сейчас особенно важно на законодательном уровне исключить возможность злоупотреблений со стороны организаций по коллективному управлению правами (играющих первостепенную роль в лицензировании): для этого необходимо обязать их принять Кодекс поведения, требования к которому разработаны уполномоченными государственными органами.

Существенную пользу принесет, с точки зрения исследователей, внедрение «расширенного коллективного лицензирования» (Extended Collective Licensing): когда организации по коллективному управлению правами имеют полномочия представлять интересы и тех авторов, которые не заключали с ними соответствующих соглашений. Подобный порядок лицензирования с 1960-х годов применяется в скандинавских странах. Он доказал свою эффективность, особенно в случаях приобретения пользователями прав на коллекции или иные большие группы результатов интеллектуальной деятельности. У правообладателей при этом должна сохраняться возможность прямо запретить коллективным организациям выдавать лицензии на их контент.

При этом отдельного обсуждения заслуживают произведения-«сироты» (владельцев прав на которые не удается установить или обнаружить). До 40% некоторых архивов Евросоюза составляют подобные произведения. Если такие работы в ближайшее время не будут оцифрованы, они могут быть утрачены навсегда. Их потеря нанесет серьезный ущерб культурному наследию Европейского Союза.

А в некоторых случаях отсутствие доступа к таким произведениям (особенно научным работам) препятствует проведению исследований, спасающих человеческие жизни (как было в истории с поиском лекарства от малярии). Предоставление доступа всем заинтересованным лицам к произведениям-«сиротам» может происходить на самых разных условиях, например, расширенного коллективного лицензирования (для использования в любых целях или, в течение

определенного срока, в социальных и культурных целях), при условии проведения предварительного «должного поиска» в базах данных объектов интеллектуальных прав, с оплатой сбора на поддержание цифровой базы данных по авторским правам и так далее.

Вознаграждение за использование таких работ должно быть номинальным, поскольку они составляют общее культурное богатство. На опасения правообладателей относительно того, что произведения-«сироты» будут в некоторых случаях более интересны пользователям, чем обычные произведения, можно ответить следующее: это хороший пример того, как всеобщие экономические интересы перевешивают возможные риски отдельных правообладателей.

Другим случаем разрешенного использования охраняемых авторским правом произведений, помимо получения лицензии, являются установленные законодательством ограничения исключительных прав, когда использование результатов интеллектуальной деятельности допускается на определенных условиях без согласия правообладателей.

Авторы с сожалением отмечают, что появление новых или изменение прежних способов использования произведений никогда не ведет к соответствующим трансформациям авторского законодательства. В результате рамки разрешенных действий с охраняемыми произведениями становятся слишком узкими и в некоторых ситуациях ограничивают применение новых цифровых технологий и инновации, ущемляют общественные интересы. Особенно в таких сферах, как обучение и научные исследования.

Еще более серьезная проблема возникает, когда люди в своей обычной жизни используют контент способами, которые, по их мнению, в принципе не могут быть запрещены: делясь с семьей понравившимися им музыкальными файлами или копируя диск, чтобы послушать его в машине. Возникает неоправданное рассогласование

между потребностями людей и нормами закона. При этом им невозможно объяснить, почему они могут свободно дать почитать любимую книгу другу, но не могут сделать того же в отношении цифровой книги или музыки. Все это подрывает уважение к закону.

В Евросоюзе действует достаточно жесткая система подобных ограничений исключительных прав, в которую включены лишь случаи свободного использования произведений в целях критики, сообщения о новостях дня, проведения исследований или архивирования. В основном в некоммерческих целях.

Более гибкая система действует в США, где судебной практикой установлена концепция «добросовестного использования» (Fair Use). Согласно концепции, суды вправе признавать те или иные действия в отношении охраняемых произведений правомерными, не дожидаясь внесения изменений в законодательство. Конечно, возможны ошибки, когда права авторов ограничиваются чрезмерно, но они также исправляются судебными решениями. В итоге открывается путь для внедрения новых технологий и появления устройств и сервисов, их использующих (в том числе в потребительской сфере, где исключения распространяются, например, на домашнюю видеозапись, кэширование результатов интернет-поиска, эскизы цифровых изображений).

Поэтому авторы исследования дают следующую рекомендацию: несмотря на возможные сложности применения концепции Fair Use, ее крайне необходимо в кратчайшие сроки внедрять в Европе. Причем делать это надо на общеевропейском уровне (изменяя законодательство ЕС) и таким образом, чтобы она распространялась на все возникающие технологические новинки (ведь сегодня им приходится ждать годами, прежде чем попасть в разряд доступных пользователям ограничений авторских прав). Концепция должна разрешать пользователям так называемое «непотребительское использование» (non-consumptive use), когда создание копий охраняемых

произведений является частью общего технологического процесса, как, например, при поисковой индексации, а не основной целью действий пользователя.

Изменение норм Евросоюза потребует длительного времени. До этого некоторые ограничения исключительных прав могут быть введены на уровне Великобритании:

– разрешение полного текстового поиска в базах данных (text mining) и в отношении охраняемых произведений при проведении некоммерческих исследований (концепция «Fair Dealing», установленная Директивой 2001/29/ЕС, здесь неприменима; ограничения должны распространяться и на коммерческие исследования, но это уже уровень Евросоюза);

– разрешение свободного копирования (private copying) произведений в личных целях (законодательство ЕС допускает такое копирование при условии выплаты компенсации, сегодня такая компенсация включается в стоимость устройств, осуществляющих копирование; представляется, что взимание такой компенсации с потребителей необоснованно, поскольку копирование является элементом обычного использования таких устройств (например, в случае записи на устройство приобретенных онлайн фильмов и музыки) и отсутствуют доказательства, что такое копирование причиняет какой-либо вред правообладателям);

– разрешение свободного преобразования формата (format shifting) правомерно приобретенного контента (например, при записи музыкальных произведений с CD на жесткий диск для их дальнейшего прослушивания на нескольких устройствах пользователя); сейчас при продаже в Великобритании программ, позволяющих изменять формат, необходимо уведомлять покупателей, что это влечет нарушение авторских прав; кажется очевидным, что правообладатели давно знают о подобных действиях пользователей (также как о

копировании в личных целях), поэтому размер вознаграждения за использование произведений, по всей видимости, устанавливается ими уже с учетом таких действий, значит, об убытках правообладателей речь вести неразумно; следовательно, пользователи должны иметь возможность свободно преобразовывать и записывать контент на различные устройства для себя и своей семьи;

– свободное изучение всех видов произведений и в любых средствах массовой информации в целях проведения некоммерческих исследований;

– свободное архивирование библиотеками любых произведений, в том числе охраняемых и сиротских (включая аудиовизуальные материалы и аудиозаписи), а также оцифровка таких произведений (подобный цифровой архив имеет колоссальную экономическую, социальную и культурную ценность);

– свободное создание пародий и стилизаций (в современных массовых сетевых коммуникациях пародии играют важную роль, давая возможность многим людям проявить свою креативность и отношение к тем или иным событиям).

На практике зачастую складывается ситуация, когда ограничения исключительных прав, установленные законом, прямо или косвенно отменяются условиями договоров, заключаемых правообладателями с пользователями. В связи с этим законодательство должно четко устанавливать, что его нормы не могут быть изменены договором.

Действительно, с одной стороны, нормы патентного права достаточно развиты, чтобы надлежащим образом защищать интересы изобретателей, производителей новой продукции и иных заинтересованных лиц (получающих доступ к сведениям о сути патентуемых объектов).

С другой стороны, из этих же положительных моментов произрастают совсем иные явления, негативно влияющие на рынок. Стремительный рост количества заявок на выдачу патентов во многих странах мира в последние годы ведет к замедлению и ухудшению качества работы патентных бюро, дублированию их усилий при рассмотрении идентичных заявок в разных странах; усложняет получение изобретателями и иными лицами достоверных сведений о содержании и объеме охраны всех действующих патентов, но при этом сокращает уровень доступных обществу научных знаний за счет выбора изобретателями не патентных форм их охраны; серьезно увеличивает транзакционные издержки и расходы на получение всех необходимых лицензий при выпуске технологически сложных устройств; лишает прибыли производителей, длительное время ожидающих выдачи патента; умножает количество судебных споров между многочисленными владельцами патентов в определенных областях.

Национальные патентные бюро должны стремиться установить тесное сотрудничество с соответствующими ведомствами в других странах, чтобы использовать единые базы данных патентуемых объектов, чтобы упростить и ускорить рассмотрение заявок.

Увеличение патентов в пересекающихся отраслях науки и техники ведет к умножению взаимозависимых патентов, непониманию того, у кого именно необходимо получать согласие на использование своего изобретения, к росту конфликтов и судебных споров, к преобладанию «оборонительного» характера патентования (вместо стимулирования инноваций), к получению низко научных патентов, к появлению «патентных пробок», когда несколько патентов разных владельцев мешают каждому из них выпускать свою продукцию, а также к злонамеренному извлечению прибыли от обладания взаимозависимыми патентами. Пример тому – производство смартфонов.

Рис. 29. Виды интеллектуальной собственности, составляющие нематериальные активы организации

Быстрее всего в последние годы растет количество патентов в сфере компьютерных технологий и телекоммуникаций. Это важно учесть, поскольку именно в отношении этих областей эксперты высказывают серьезные сомнения, что патентование поддерживает инновации. Изобретения в указанных сферах чаще всего логически следуют из уже имеющихся изобретений и инноваций, нежели чем представляют новое слово в науке и технике. В результате поддержка инновациям оказывается слабой, а патенты образуют собой целые «заросли», естественно, препятствующие рыночному росту.

Но пока нет еще единого способа решить проблему патентных «зарослей». Участники рынка сами применяют достаточно разнооб-

разные методы наведения порядка: создавая стандарты, патентные пулы и так далее.

Государству в этой связи рекомендовано предпринять следующие три шага: предотвращение распространения патентования на те сферы бизнеса, где стимулирующая роль патентов ниже в сравнении с создаваемыми накладными расходами; увеличение суммы пошлин за поддержание патентов в силе; обеспечение выдачи патентов только высокого качества.

Кроме того, эффективные меры преодоления негативных последствий патентования уже применяются внутри рынка: кросслицензирование, патентные пулы, открытые технологически стандарты тому пример. Эти подходы требуют одобрения основными участниками бизнеса. Помощь им (в установлении размера роялти и т.п.) могут оказать органы по стандартизации. Однако данные методы не всегда распространяются на предприятия малого и среднего бизнеса или не могут быть поддержаны ими по экономическим соображениям. Что затрудняет для них доступ на соответствующие рынки.

Также данные методы иногда недобросовестно используются различными так называемыми «не практикующими организациями» (non-practising entity, NPE) или попросту «троллями», приобретающими патенты исключительно с целью получения средств за их использование от производителей.

В связи с изложенным подобные методы представляют вполне разумными, но недостаточными для решения всех сложностей, что требует дополнения их иными государственными мероприятиями.

Авторы Доклада уверены, что патентование компьютерных программ практически не стимулирует инновации, существенно увеличивает транзакционные издержки, взращивает непроходимые «заросли» патентов.

В Европе, в отличие от Японии и США, предъявляются более жесткие требования к компьютерным программам, которые могут быть запатентованы: если программы привносят «технический вклад» (управляют роботами или делают внутренние операции компьютера более эффективными), то на них возможна выдача патента, если же программы имеют общее применение («не технические программы», «non-technical computer programs»), например, осуществляют обработку текста, то патенты не выдаются.

Хотя Европейское патентное ведомство изначально исходило из тех же принципов, что и Ведомство по интеллектуальным правам Великобритании, в последние годы оно все чаще выдает патенты на не технические программы. В этой связи эксперты рекомендуют британскому бюро придерживаться своей политики и стараться убедить европейских коллег отказываться от патентования не технических программ.

По тем же соображениям не следует выдавать патенты на различные «бизнес методы» (такие как маркетинговые и ценовые схемы). Сегодня в Европе отказывают в их патентовании, хотя в США преобладает противоположный подход.

Что же касается предложения воздействовать пошлинами на патентное поведение, то основная цель данного метода – побудить владельца патента оценить экономическую выгоду от обладания патентом и, в случае ее недостаточности, отказаться от сохранения его в силе. Пошлины за поддержание действия патента, увеличивающиеся за каждый последующий год, могут быть замечательным средством для этого. Для предприятий SME могут быть установлены льготы.

В Докладе рассмотрены также проблемы **дизайна**. Дизайн – очень широкое понятие, включающее различные сферы производства от дизайна одежды до промышленного ди-

зайна. При этом он составляет существенную часть нематериальных инвестиций в британской экономике (в 2008 году инвестиции в дизайн оценивались в 1,6% ВВП Великобритании).

Авторы отмечают, что основная проблема в правовом регулировании дизайна состоит в разнообразии вариантов такого регулирования, порождающем сложность выбора способа охраны и защиты прав авторов. Так, создатели объектов дизайна могут претендовать на особые «права на дизайн» (при этом охрана допустима как при регистрации объектов на уровне Великобритании или ЕС, так и без такой регистрации), на авторские права или права на товарные знаки. Права на дизайн чаще касаются технического дизайна, тогда как авторские права – художественного дизайна, например, иллюстраций. Авторские права могут защищаться в порядке уголовного преследования, тогда как права на дизайн – только гражданского. Различаются сроки действия прав и их объем.

Словом, пока не проведено более пристальное изучение связанных с дизайном вопросов, нельзя однозначно сформулировать рекомендации по улучшению его правового регулирования.

Тем не менее эксперты уверены, что некоторые вышеперечисленные рекомендации (в виде внесения информации обо всех объектах в единый цифровой реестр и т.п.) могут быть вполне применимы. Затягивать с изучением этой сферы творчества не стоит, поскольку и здесь развитие технологий способно причинить серьезные трудности как правообладателям, так и пользователям. Авторы отчета напоминают, что приближающееся массовое внедрение 3D печати (3D printing) и другие инновации способно серьезно повлиять на всех участников рынка, поэтому крайне важно подготовиться к этому заранее.

Эксперты в целом убеждены, что ситуация, когда права невозможно реализовать или защитить, горазда хуже той, когда права не предоставлялись вовсе. Авторы, разработчики и иные правооблада-

тели вкладывают свои усилия, исходя из определенных ожиданий. Если они не оправдываются, ущерб наносится творчеству, инновациям и социальному порядку.

Особое внимание правообладатели обращают на онлайновые нарушения принадлежащих им прав, которые приобрели сегодня массовый характер, поскольку опасаются, что они приведут к краху их бизнеса.

Масштаб нарушений связан с легкостью и бесплатностью процесса копирования и распространения произведений, достаточной анонимностью действий в интернете, а также уверенностью многих пользователей в том, что их определенные действия являются правомерными. Так, согласно исследованию Consumer Focus, опубликованному в феврале 2010 года, 73% потребителей не знают, что авторское законодательство не разрешает копировать или записывать. 44% peer-to-peer пользователей убеждены, что их действия правомерны. А многие вообще не считают пиратство этической проблемой.

Оценки уровня пиратства у разных исследователей очень сильно разнятся, ведь единых методик пока не разработано, поэтому к полученным ими результатам надо относиться с осторожностью. Согласно отчету BPI «Digital Music nation», в 2010 году объем нелегального скачивания музыкальных произведений в Великобритании составил 65% от общего объема загрузок, тогда как в отчете Midemnet «2010 Global Music Study» уровень пиратских скачиваний оценен в 13%.

В отчете приводится таблица данных по уровням пиратства, собранных различными исследователями, показывающая, что и в отношении иных объектов интеллектуальной собственности согласие далеко не достигнуто

Приведем некоторые цифры.

1) Уровень пиратства в отношении художественных фильмов, телевизионных программ:

– 2010 год: 14% пользователей нелегально загружают фильмы и программы через P2P сервисы;

– 2008–09 годы: 29% потребителей смотрят пиратские DVD, 21% скачивают нелегальные файлы.

2) В отношении игр, программного обеспечения:

– 2008–09 годы: 14–16% пользователей, соответственно, пересылают (file-sharing) нелегальные файлы;

– 2007–08 годы: в Европе 35–40% пользователей, соответственно, владеют хотя бы одной нелегальной копией игры.

3) В отношении книг:

– 2010 год: 10% от общего объема продаж в США приходились на контрафактные экземпляры.

4) В отношении нелегального контента в целом:

– апрель 2011 года: свыше 45 миллионов уникальных пользователей за месяц скачивали пиратский контент с 15 наиболее популярных торрент-сайтов;

– 2010 год: за год совершено более 778 миллионов нарушений авторского права в цифровой сфере;

– 2008–09 годы: от 34 до 70% мирового трафика приходилось на передачу нелегального контента, в зависимости от региона.

При этом общее влияние пиратства на состояние экономики оценить крайне сложно, поскольку, как уже говорилось, нет ни авторитетных методик, ни точных цифр. Тем не менее исследователи приняли во внимание все доступные им отчеты и рассчитали приблизительные средние значения. Получилась следующая картина,

общая и для Великобритании, и для Евросоюза, и для мира в целом: на нарушения авторского права приходится менее 0,1% от объема экономической деятельности. А общая доля нарушений в сфере интеллектуальной собственности составляет от 0,1 до 0,5% экономической деятельности. Как видим, данные цифры не являются ни слишком маленькими, ни излишне большими.

В сравнении с иными странами уровень пиратства в Великобритании сравнительно невелик: доля скачивания нелегального контента составляет 15%, тогда как, например, в Китае – около 70%.

Если оценивать убытки от пиратства не в общем объеме экономической активности, а в творческих сферах производства, то можно принять во внимание авторитетное исследование Business Action to Stop Counterfeiting and Piracy (BASCAP): в нем сделан вывод, что ущерб от пиратства равен 1,24% от общего вклада основных отраслей, связанных с авторским правом, в экономику Великобритании. При этом авторы рассматриваемого отчета уверены, что эта цифра представляет собой максимальный предел возможного диапазона, тогда как среднее значение гораздо меньше.

В дополнение эксперты проанализировали уровни продаж различных результатов интеллектуальной деятельности, чтобы оценить влияние на них контрафактных материалов. Было установлено, что:

– средний уровень доходов музыкальной индустрии, несмотря на действия пиратов и серьезные убытки отдельных компаний, продолжает расти – в 2009 году на 5% по сравнению с 2008 годом, – прежде всего за счет живых исполнений, роста международного лицензирования и некоторой стабилизации на рынке звукозаписи;

– продажи в издательском бизнесе также либо растут, либо сохраняют свои показатели в течение 2004–2009 годов;

– видеосектор также сохраняет уровень доходов стабильным,

причем несмотря на рецессию в Европе и Северной Америке.

Тем не менее исследователи зафиксировали сокращение финансирования новых проектов в творческих сферах экономики. Чаще всего оно вызывается опасениями относительно возможного влияния пиратства на будущие доходы и инвестиции. Хотя достоверно установлено, что нарушения интеллектуальных прав оказывают не столь губительное воздействие на экономические результаты, как это иногда преподносится.

Относительно предложений по борьбе с пиратством, поступающих от правообладателей и организаций по коллективному управлению правами, авторы отчета поясняют следующее. Чаще всего предложения сводятся к ужесточению санкций за совершение нарушений, хотя эффективность подобных мер достаточно низка.

Авторы ссылаются на заключение американского US Social Science Research Council (SSRC), в котором эта ситуация рассматривается детально. Так, была изучена эпопея с 27 000 судебными делами по искам звукозаписывающей ассоциации RIAA к пользователям P2P-сервисов в период с 2003 по 2008 год. Вскоре после начала предъявления исков и публичного оповещения об этом использование P2P-сервисов сократилось на 50% (с 29 до 14%). Но уже к 2005 году почти вернулось к прежнему уровню, достигнув 24%. Результаты массированного судебного преследования и закрытия пиратских сайтов весьма скромны, поскольку стоимость обслуживания торрент-трекеров и индексирующих сайтов крайне мала и на месте блокированных сайтов достаточно быстро возникают новые.

Сложно оценить эффективность и французского закона HADOPI (о блокировании доступа к интернету злостным нарушителям после трехкратного предупреждения): половина из опрошенных нарушителей заявила, что не намерена менять свое поведение, треть согласна отказаться от незаконных действий, при этом четверть об-

щего количества опрошенных от ответа воздержалась.

Различные образовательные кампании, прежде всего направленные на молодых людей, крайне редко меняют их отношение к пиратству. Образовательные программы могут полезны, если они сопровождаются улучшением правоприменения и предоставлением пользователям широкого выбора доступного легального контента.

Эксперты отмечают, что наиболее эффективным методом борьбы с пиратством надо признать именно создание достаточного количества сервисов, предлагающих пользователям легальный контент на понятных условиях и по доступной цене.

Авторы приводят любопытные данные из отчета BPI Digital Music nation 2010 года. В ходе данного исследования пользователи, отказавшиеся от использования P2P, были опрошены о причинах их выбора: 29% заявили, что они нашли более удобные платные сервисы; 24% – что сочли это нечестным по отношению к артистам и авторам; 23% – стали использовать бесплатные потоковые сервисы; 21% – ищут музыку в социальных сетях; 16% – используют форумы и блоги; 13% – уже загрузили почти все, что хотели; 12% – были обеспокоены, что их могут поймать; 12% – признали неправильным использовать сервисы с пиратским контентом.

Возможные возражения некоторых правообладателей, что они не в состоянии конкурировать с бесплатным распространением их контента, опровергаются статистикой, показывающей, что многие пользователи готовы платить за получения контента разумное вознаграждение, если сам порядок получения достаточно прост.

Повышение эффективности правоприменения напрямую зависит от доступности всем участникам рынка судебной защиты. Высокие пошлины за рассмотрение споров в сфере интеллектуальных прав, существующие в Великобритании, удерживают многих предпринимателей, в особенности из малого бизнеса, от обращения в суды.

Одним из позитивных шагов в этом направлении авторы называют недавнее создание Патентных судов графства (Patents County Courts), рассматривающих несложные дела в сфере авторского и патентного права, товарных знаков и дизайна. К сожалению, сегодня далеко не все представители бизнеса знают о существовании таких судов.

В России вопросы защиты ИС находятся в компетенции нескольких государственных органов: Роспатента, Минэкономразвития, Минобрнауки. В последние годы было усовершенствовано законодательство в этой сфере, с 2013 года начали работу арбитражные суды по ИС, ужесточаются меры ответственности за ее кражу.

Но пока госрегулирование в этой сфере не всегда соизмеряется с международными стандартами. Патенты официально не публикуются в форме открытых данных, а регистрация ИС – это долговременный процесс, который не отвечает реалиям цифровой экономики. В сфере защиты авторского права действует «антипиратский» закон, но полностью контролировать нелегальный контент пока не удается.

Так, в 2018 году была принята Стратегия научно-технологического развития России, которая предусматривает организацию системы технологического трансфера, управления, охраны и защиты интеллектуальной собственности.

Действует также Национальная интеллектуальная инициатива (НИИ) – комплекс мер, направленных на создание конкурентоспособного рынка ИС и открытого цифрового рынка интеллектуальных прав. В рамках НИИ разрабатывается дорожная карта IPnet и открытая общественная сетевая платформа для управления интеллектуальной собственностью на базе технологии блокчейн. При этом подчеркнем, что обеспечение прав России на ИС внутри страны и за рубежом является важным компонентом развития системы ИС. В этом году Российский экспортный центр, Роспатент и фонд «Ин-

нопрактика» должны разработать концепцию и план мероприятий по созданию центров защиты ИС в зарубежных странах.

Вопросы для закрепления изученного материала

1. Понятие «информационная безопасность».
2. Понятие конфиденциальности информации.
3. Свойства информации с точки зрения ее безопасности.
4. Содержание системы информационной безопасности.
5. Угрозы информационной безопасности.
6. Контур информационной безопасности.
7. Подходы к построению системы обеспечения информационной безопасности.
8. Система информационной безопасности предприятия.
9. Анализ и оценка рисков информационной безопасности.
10. Порядок применения программы управления рисками в системе информационной безопасности по методике Microsoft.
11. Методика «CCTA Risk Analysis and Management Method (CRAMM)».
12. Методика «Facilitated Risk Analysis Process (FRAP)».
13. Программа Risk Advisor.
14. ГРИФ – российское комплексное средство анализа и управления рисками информационной системы организации.
15. Модель анализа угроз и уязвимостей.
16. Средства защиты информации.
17. Аппаратные (технические) средства защиты информации.
18. Программные средства защиты информации.
19. Антивирусные программы.
20. Профилактика заражения компьютера.

21. Криптографические средства защиты информации.

22. Защита информации от несанкционированного доступа.

23. Понятие «цифровая подпись».

24. Средства электронной цифровой подписи.

25. Схема функционирования ЭЦП.

26. Роль ЭПЦ в электронном документообороте.

27. Правовая защита информации в цифровой экономике.

28. Правовая защита интеллектуальной собственности в цифровой экономике.