МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАФЕДРА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И ПРОГРАММИРОВАНИЯ

АКТУАЛЬНЫЕ ВОПРОСЫ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Под редакцией д-ра экон. наук, проф. Е. В. Стельмашонок

**ИЗДАТЕЛЬСТВО
САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО
ЭКОНОМИЧЕСКОГО УНИВЕРСИТЕТА
2015**

ББК 32.81
А43

А43 Актуальные вопросы безопасности современных информационных технологий / под ред. д-ра экон. наук, проф. Е. В. Стельмашонок. – СПб. : Изд-во СПбГЭУ, 2015. – 164 с.

ISBN 978-5-7310-3418-0

Монография посвящена проблемам информационной безопасности и методам защиты информации в компьютерных системах. Особое внимание уделено методам исследования защищенности и поиска уязвимостей компьютерных систем. Монография может быть полезна магистрантам, аспирантам и специалистам в области информационных технологий, а также всем, кто интересуется вопросами обеспечения информационной безопасности.

The monograph is devoted to problems of information security and information protection methods in computer systems. Particular attention is paid to research methods of security and vulnerability assessment of computer systems. The monograph can be useful to undergraduates, graduate specialists in information technology, as well as all those interested in questions of information security.

ББК 32.81

Коллектив авторов:
Р. Р. Бежан (п. 2.2), **А. Г. Боховко** (п. 1.1), **В. Н. Бугорский** (п. 4.1–4.3), **О. Д. Быстрова** (п. 2.4), **И. Н. Васильева** (п. 3.1–3.3), **И. Г. Гниденко** (п. 1.2), **Л. А. Еникеева** (п. 4.4), **М. С. Медведев** (п. 2.3), **О. Д. Мердина** (п. 1.2), **С. К. Морозов** (п. 2.6), **С. О. Семенова** (п. 3.3), **Е. В. Стельмашонок** (п. 4.1–4.3), **Д. Ю. Федоров** (п. 2.5), **Г. М. Чернокнижный** (п. 1.1), **Е. В. Черток** (п. 2.1), **М. С. Ширшикова** (п. 4.4)

Рецензенты: зав. кафедрой интеллектуальных систем и защиты информации СПбГУПТД, д-р техн. наук, проф. **А. Г. Макаров**
зав. кафедрой информатики СПбГЭУ заслуженный деятель науки РФ, д-р техн. наук, проф. **В. В. Трофимов**

ISBN 978-5-7310-3418-0

ОГЛАВЛЕНИЕ

Глава 1. МЕТОДЫ АУТЕНТИФИКАЦИИ И РАЗГРАНИЧЕНИЯ ДОСТУПА

1.1. Аутентификация в информационных системах: как это есть и как это должно быть

Аутентификация пользователей является важной частью безопасности информационных систем, наряду с конфиденциальностью и целостностью [1]. На сегодняшний день в большинстве информационных систем популярным методом подтверждения подлинности является примитивный способ парольной аутентификации «на основе знания чего-либо» с использованием пары «логин–пароль».

Главным достоинством парольной аутентификации является простота, привычность и удобство использования. Теоретически этот способ является безопасным, так как современные протоколы аутентификации обладают необходимой криптостойкостью. На практике парольный способ имеет ряд серьезных недостатков при его неправильном использовании и несоблюдении парольных политик. Степень удобства пароля для пользователя зависит от того, легко ли запомнить пароль и затем набрать его на клавиатуре. По этой причине большинство пользователей в качестве пароля выбирают короткие и легко запоминаемые последовательности символов. Это могут быть имена, даты рождения пользователей или такие цифровые последовательности, как «12345».

По результатам статистики компании Positive Technologies в большинстве российских компаний 52% паролей пользователей состоят только из цифр, по 17% паролей содержат только символы английского алфавита в верхнем или нижнем регистре. Также статистика показала, что в большинстве случаев длина пароля не превышает 8 символов.

Таким образом, около 88% паролей пользователей российских компаний позволяют с высокой долей вероятности успешно проводить атаки на подбор пароля в тех случаях, когда не используются различного рода превентивные механизмы, затрудняющие реализацию этой атаки [2].

О низкой безопасности паролей, которые выбирают пользователи, написано много статей. Самая старая была написана Даниелем Клейном в 1990 г. В ней автор описывает эксперимент, в котором у него с помощью словаря из примерно 63 000 слов получилось за пару недель подобрать пароли к 25% учетным записям пользователей. Стоит отметить, что, согласно статистике Positive Technologies, люди не используют сложные пароли до сих пор. Также, согласно закону Мура, вычислительные мощности компьютеров выросли к настоящему времени более чем в 16 тысяч раз [3].

Брюс Шнайер отметил, что величина, определяющая криптостойкость пароля – это количество операций, требуемых для анализа всех вариантов [4]. Поэтому, чем больше вариантов для подбора пароля предлагается, тем дольше злоумышленник будет подбирать пароль. Отсюда следует необходимость соблюдения парольных политик.

Однако когда парольные политики все-таки применяются, это приводит к усложнению паролей и затрудняет их запоминание пользователями. Делает проблему еще более сложной и тот факт, что у каждого сотрудника любой компании наберется с десяток паролей к разным вебсервисам и информационным системам. В таком случае многие пользователи находят выход в записывании сложных последовательностей на бумагу, которую хранят рядом с рабочей станцией. Это также подрывает безопасность, ради которой создавались парольные политики. Несмотря на большие усилия специалистов по информационной безопасности в вопросе обязательной работы с персоналом, на практике лишь немногие компании тратятся на тренинги и устраивают проверки выполнения установленных требований политик ИБ. Свод этих политик, единожды утвержденный начальством, скорее всего, заперт в сейфе службы безопасности и не является в общепринятом смысле «рабочим» документом. Также существует большое количество возможных атак на пароли, использующих человеческий фактор:

1. Полный перебор (Brute Force) – самый простой метод, заключающийся в переборе всех комбинаций символов. Чем длиннее пароль, тем больше времени и вычислительной мощности потребуется злоумышленнику, чтобы его подобрать.
2. Атака по словарю – из заранее подготовленного словаря автоматически проверяются слова или последовательности символов, которые наиболее часто выбираются в качестве пароля.
3. Сброс пароля с помощью внешнего носителя.
4. Захват паролей с помощью вредоносного программного обеспечения.
5. Регистрация излучения путем перехвата информации с монитора.
6. Социальный инжиниринг – способ кражи пароля или доступа в информационную систему, основанный на особенностях психологии человека.
7. Фишинг – способ кражи паролей с помощью подставных сайтов.

На данный момент средства парольной аутентификации являются самыми экономичными по стоимости, но одновременно и наименее безопасными. Парольная защита не удовлетворяет современному уровню требований информационной безопасности. Надежность этого способа аутентификации в значительной степени зависит от человеческого фактора. Немного улучшают ситуацию регулярные семинары для сотрудников,

направленные на повышение их грамотности в вопросах информационной безопасности, с обязательным запугиванием на тему ответственности за разглашение пароля и т. д. Любые внезапные проверки просто заставят работников отлепить стикеры с паролями от монитора и поместить их под клавиатуру или в лучшем случае – в ящик стола.

Учитывая быстрый рост рисков современных угроз – как внешних, так и внутренних – пренебрегать организацией защиты доступа к информационным ресурсам, критически важным для работы любой компании – означает фактически открыть двери злоумышленникам и ждать прецедента. Компании, пытающиеся решить эту проблему с помощью парольных политик, просто тешат себя напрасными надеждами.

Все перечисленные недостатки паролей значительно снижают степень безопасности системы и позволяют осуществить несанкционированный доступ к информации различного уровня конфиденциальности. Хотя против каждой атаки существуют свои методы защиты, однако эти методы также имеют недостатки. Такой метод защиты, как парольные политики, создают неудобства для пользователей, а борьба с электромагнитным излучением – достаточно дорогая процедура. Одно из решений борьбы с разным родом атак на пароли – это не аутентификация, построенная на многоразовом пароле, а переход на одноразовые пароли.

Одноразовые пароли (OTP, One Time Passwords) – информация для единичного использования, получаемая с помощью программно-аппаратных устройств.

Одноразовые пароли решают ряд проблем, присущих фиксированным паролям. Их применение стало большим шагом вперед. Если злоумышленник узнает одноразовый пароль, то вероятность, что он сможет повторно воспользоваться им низкая, так как этот пароль актуален на протяжении какого-то короткого промежутка времени. Для генерации одноразовых паролей обычно используют аппаратные устройства, например OTP-токен, или приложение, установленное на смартфон.

Таким образом, использование одноразовых паролей, по сравнению со стандартной парольной аутентификацией, является аутентификацией с помощью другого фактора аутентификации – аутентификация «на основе обладания чем-либо» или на основе программно-аппаратной аутентификации.

Системы аутентификации, построенные по принципу «чем вы обладаете», предоставляют больше возможностей для усиления защиты. Данный метод аутентификации решает проблему запоминания пользователем сложных паролей, предоставляя возможность генерирования одноразовых паролей или записи в защищенную память аппаратного устройства (смарт-карта, USB-ключ и др.) паролей, закрытых ключей и сертификатов.

В процесс аутентификации входят программные и аппаратные аутентификаторы, устройства ввода-вывода: ридеры, считыватели, адаптеры, разъемы и другие устройства, а также соответствующее программное обеспечение. Аутентификаторы хранят секретные данные, необходимые для процесса аутентификации пользователя, в защищенной памяти. Программное обеспечение и устройства ввода-вывода отвечают за обмен этой информации между аутентификатором и защищаемой системой. Аутентификационные секретные данные предъявляются системе в виде цифрового кода.

По способу обмена секретными данными между аутентификатором и устройствами ввода-вывода аппаратные устройства аутентификации делятся на:

- контактные;
- бесконтактные;
- комбинированные.

Для построения системы аутентификации на базе аппаратных аутентификаторов используются:

- USB-ключи;
- OTP-токены (программные и аппаратные);
- смарт-карты;
- Touch Memory (информационная «таблетка»);
- радиочастотные идентификаторы (RFID).

К контактным идентификаторам относят Touch Memory, контактные смарт-карты и USB-ключи. Работа контактных устройств считывания аутентификационных данных основана на непосредственном взаимодействии идентификатора и устройств ввода-вывода: проведение идентификатора через считыватель, фиксирование идентификатора в считывателе или простое соприкосновение этих устройств.

Для бесконтактного или дистанционного способа считывания не требуется четкого фиксирования или соприкосновения идентификатора и считывателя. Для считывания данных необходимо, чтобы устройство попало в поле считывающего устройства или устройство необходимо поднести на определенное расстояние к считывателю. К бесконтактным идентификаторам относят смарт-карты на основе RFID-меток. OTP-токены являются особым случаем бесконтактного способа обмена секретными данными, так как пользователь вводит сгенерированный одноразовый пароль вручную и при этом не используются никакие считыватели.

Комбинированный способ предполагает сочетание обоих методов. Примером комбинированного устройства могут быть смарт-карты.

Согласно комплексному подходу к обеспечению информационной безопасности, организационные мероприятия необходимо дополнять со-

ответствующими техническими мерами. Отказ от слабых паролей в пользу двухфакторного метода аутентификации на базе аппаратных токенов признан наиболее популярным способом решения данной задачи на сегодняшний день.

Двухфакторный способ подтверждения подлинности аутентификационных данных основан на следующих факторах – «на основе знания чего-либо» и «на основе обладания чем-либо». Для доступа в систему пользователь в первую очередь обязан предъявить нечто – обычно это токен или смарт-карта, которые подтверждают факт обладания, а затем доказать, что это устройство действительно принадлежит ему, указав пароль или PIN-код к нему.

Подобные технологии позволяют повысить уровень информационной безопасности в компании и существенно облегчить жизнь ее сотрудникам. На одном устройстве можно хранить пароли ко всем системам и приложениям (политика единого входа – Single Sign On), с которыми ежедневно приходится работать пользователю.

Статистика показывает, что к физическому носителю парольной информации сотрудники компаний относятся во много раз ответственнее, чем к абстрактному паролю. Психологическая тонкость состоит в том, что устройство выдается под расписку, сотрудник несет за него материальную и, своего рода, моральную ответственность. Кроме того, устройство персонализировано, а, следовательно, все действия с его использованием будут выполняться от лица владельца этого устройства и могут быть отслежены в системе.

В правильно спроектированную систему двухфакторной аутентификации можно заложить и другие полезные возможности. Например, встроить в устройства аутентификации RFID-метки, которые служат для прохода через систему контроля и управления доступом (СКУД), что позволит обеспечить политику «чистых экранов», заключающуюся в том, что пользователь не может выйти из помещения (покурить, попить чаю и т. д.), не извлекая устройство из компьютера. В момент извлечения операционная система блокируется до следующего подключения с вводом PIN-кода [5].

Еще один фактор, который может использоваться для построения двухфакторной системы аутентификации – это «то, что является частью меня». Биометрическая характеристика – уникальная измеримая черта человека, использующаяся для установления личности. Разделяют физиологические и поведенческие характеристики. Физиологические характеристики основаны на анатомических характеристиках человека, а поведенческие – на измерениях действий человека. Большая часть физиологических характеристик не меняется со временем. Исключение составляют черты лица, которые могут измениться с возрастом или с поведением че-

ловека. Поведенческие характеристики меняются из-за болезни, под влиянием стресса, поэтому они не стабильны и обеспечивают менее качественную аутентификацию.

Обычно процесс биометрической аутентификации является самым простым и удобным для пользователя. Смарт-карту или USB-ключ можно забыть дома, с биометрическими характеристиками такого не произойдет. Биометрические характеристики человека уникальны и неизменны с возрастом (физиологические характеристики), их нельзя передать другому пользователю, что в теории позволяет говорить о надежности биометрической системы. Однако на сегодняшний день существует много проблем с реализацией биометрических систем.

Несмотря на то, что биометрические системы отличаются способами измерений биометрических характеристик, они работают по одному принципу. Пользователю необходимо предоставить образец. Это может быть отпечаток пальца, запись голоса и т. д. Далее регистрирующее устройство обрабатывает предоставленную информацию для выделения отличительных характеристик. В итоге формируется контрольный шаблон, состоящий из довольно больших числовых последовательностей. Восстановить первоначальный образец из такой последовательности – крайне тяжелая задача. Созданный контрольный шаблон является паролем пользователя. Он сверяется с эталонным шаблоном, созданным заранее в результате нескольких образцов при регистрации пользователя. Из-за того, что контрольный и эталонный шаблоны никогда не совпадают на 100%, вводится понятие настраиваемой пороговой величины. Биометрическая система должна принять решение – достаточно ли совпадают эти шаблоны для успешной аутентификации. Вводятся два параметра:

1) FAR (False Accept Rate) – вероятность ошибочного допуска;
2) FRR (False Reject Rate) – вероятность ошибочного отказа в доступе.

Системы с низким значением FAR более защищены, тогда как системы с низким значением FRR более просты в использовании. Существует правило: чем ниже FAR, тем выше FRR. Поэтому безопасность зачастую конкурирует с простотой использования.

Простота регистрации и качество шаблонов – два важных фактора общей эффективности биометрической системы. Некачественный шаблон может осложнить работу пользователя, вынуждая его прибегнуть к повторной регистрации в биометрической системе. Качественно спроектированная биометрическая система в большинстве случаев правильно выполняет аутентификацию.

Главный недостаток относится к считывателям биометрических характеристик, качество и точность сканирования которых напрямую зависит от их стоимости. Например, в случае со сканированием отпечатков

пальцев могут использоваться оптические сканеры, которые формируют качественное изображение, но требовательны к чистоте пальцев. Электронные сканеры, в свою очередь, менее надежны, однако могут распознавать загрязненные отпечатки пальцев. Также к недостаткам считывателей относится крайне сложная настройка FAR и FRR параметров. Приходится делать выбор между удобством использования системы и ее безопасностью.

Недостатки самих биометрических характеристик создают следующие проблемы:

- хищение злоумышленником шаблонов биометрических характеристик делает невозможным их замену;
- использование одних и тех же биометрических характеристик в разных системах повышает риск их утечки или кражи. Так, например использование отпечатков пальцев на предыдущих местах работы может использоваться злоумышленником для своих целей.

Кроме недостатков с технической стороны, биометрия имеет ряд других. Возникает вопрос вмешательства в частную жизнь, личные, культурные и религиозные аспекты, также вопросы гигиены и травмоопасности. Действительно, пользователям не безразличен факт хранения и распространения их биометрических данных. Они не имеют возможности контролировать распространение таких данных, поэтому опасаются злоупотреблений. Еще один немаловажный факт: будет ли прибор для считывания, например геометрии руки, обрабатываться раствором после каждого использования. Прибор может нанести пользователю травму, например, система сканирования сетчатки, в которой свет направляется в глаза. Также пользователи подвергаются риску причинения вреда со стороны преступников – потеря части тела. Непригодность для всех пользователей – еще один минус биометрической аутентификации. Существует вероятность, что пользователь может не иметь необходимых частей тела для внесения в систему биометрического параметра. Для людей, которые носят линзы, сканирование радужной оболочки глаза будет неудобной процедурой, люди с артритом не смогут ровно приложить палец к считывателю, что затруднит процесс аутентификации и т. д.

Специалисты предрекают биометрическим системам большое будущее, но существует большое количество проблем, которые ставят под сомнение целесообразность их использования. Есть вероятность, что со временем и с развитием технологий эти проблемы исчезнут. Создание концепции Match-on-card в 2013 г. стало большим шагом вперед и сейчас используется все чаще.

Сегодня существует большое количество компаний, занимающихся вопросами контроля доступа. В частности, под торговой маркой Smartec на российский рынок поставляется широкий спектр оборудования, в том

числе биометрического, для построения системы контроля доступа разной конфигурации и сложности. Для построения такой системы предлагаются различные Proximity карты, брелоки и считыватели стандарта EM Marine, считыватели отпечатков пальцев. Можно привести примеры наиболее интересных, по мнению авторов, устройств, удовлетворяющих критерию «цена-качество».

Биометрический считыватель контроля доступа ST-FR020EM (рис. 1.1) позволяет проверять подлинность персонала по отпечаткам пальцев и по Proximity картам стандарта EM Marine. Может использоваться для построения автономной системы контроля доступа, а также существует возможность интеграции в различные СКУД, при этом их программирование выполняется с помощью специализированного ПО. Считыватель рассчитан на обслуживание до 1 500 шаблонов отпечатков пальцев, при этом на каждого человека можно завести до 10 отпечатков пальцев. Есть возможность подключения дополнительных Proximity или биометрических считывателей. Обеспечивает приемлемое (<1 с) время идентификации в диапазоне температур от -10 до +50°С. Цена устройства: $165 [6].

Рис. 1.1. Биометрический считыватель контроля доступа ST-FR020EM

Более «старшие» (и дорогие) модели имеют расширенный диапазон обслуживания по числу шаблонов, возможность подключения внешних сигнальных и исполнительных устройств, средства термостатирования для работы в уличных условиях, совместимы со СКУД других производителей. Вероятностные оценочные параметры этих устройств находятся на достаточно высоком уровне:

- FAR: <0.0001%;
- FRR: <1%.

Интерес представляет биометрический считыватель идентификации по лицу ST-FR040EM (рис. 1.2), который может проверять подлинность персонала по геометрии лица и/или по Proximity картам стандарта EM Marine.

Рис. 1.2. Считыватель идентификации по лицу ST-FR040EM

Используется в системах контроля доступа и учета рабочего времени. Устройство поддерживает такие режимы распознавания пользователей, как аутентификация по лицу, по карте, по коду, или их любые логические комбинации. Регистрация прихода и ухода с работы осуществляется с помощью одного сканера/считывателя, в этом случае для выбора типа события (приход/уход на перерыв/с перерыва) используется дополнительное нажатие экранных функциональных кнопок. Цена считывателя: $425 [6].

Из недорогих устройств ($90) отметим USB сканер отпечатков пальцев ST-FE700 (рис. 1.3).

Рис. 1.3. Сканер ST-FE700

Возможно его использование совместно с различными программными приложениями для ввода в базу шаблонов отпечатков пальцев, при этом для интеграции с ПО сторонних производителей можно использовать SDK. Аппаратная часть ST-FE700 обеспечивает автоматическую калибровку считывателя и осуществляет шифрование данных при их передаче через USB интерфейс.

Новым стандартом в области систем контроля доступа являются решения на платформе iCLASS SE от HID Global. iCLASS SE обеспечивает:

- повышенную безопасность;
- повышенную конфиденциальность;
- гибкость;

- функциональность;
- повышенную мобильность.

Платформа содержит широкий ассортимент считывателей, смарт-карт и цифровых мобильных средств доступа. Представленные в платформе iCLASS Seos средства аутентификации можно использовать в мобильных устройствах, поддерживающих беспроводную связь малого радиуса действия (NFC), чтобы с помощью смартфонов получать доступ к различным ресурсам. Платформа гарантирует более надежную защиту идентификационных данных, дополнительную диверсификацию ключей, аутентификацию и шифрование. В платформе используются современные методы криптографии и защищенный протокол обмена сообщениями [7].

Как мы видим, сегодня на смену паролям предлагается довольно много других способов проверки подлинности, которые значительно повышают безопасность входа в систему по сравнению с парольной аутентификацией.

В случае использования смарт-карт или USB-ключей безопасность процесса аутентификации обеспечивается за счет использования криптопроцессоров и алгоритмов шифрования, в случае использования OTP-токенов – за счет одноразовых паролей. Тем самым большая часть ответственности за безопасное хранение, передачу и генерацию секретных данных перекладывается на аппаратное устройство. Обязанность, которая ложится на пользователя, – это бережно хранить аутентификатор, что намного проще, чем запоминать длинный и сложный пароль. Если все-таки пользователь не справляется со своей обязанностью, т. е. происходит кража или потеря аутентификатора, то обнаружить его пропажу гораздо проще, чем обнаружить кражу пароля. После нескольких неудачных попыток злоумышленника подобрать PIN-код вручную устройство блокируется. Следовательно, все это дает дополнительное время администратору информационной безопасности для принятия экстренных мер по блокированию учетной записи данного пользователя.

Еще более эффективным является применение двух взаимодополняющих друг друга факторов проверки подлинности, что обеспечивает защиту от атак на один фактор. Второй фактор является дополнительной мерой защиты информационной системы, который доставляет злоумышленнику дополнительные трудности при попытке несанкционированного доступа, и он должен очень постараться, чтобы обойти такую аутентификацию. Фактически сложность этой задачи намного выше, а вероятность успеха намного ниже, поэтому злоумышленнику экономически выгодно сосредоточится на более простых решениях кражи необходимой информации. По этой причине число взломов систем с двухфакторной аутентификацией на сегодняшний день ничтожно мало. Чем больше факторов используется для построения многофакторной процедуры аутентифика-

ции, тем надежнее система. Однако не стоит забывать и о том, что у пользователя прохождение такой процедуры будет отнимать много времени и, следовательно, доставлять неудобства. Также при использовании большого числа факторов сильно возрастает цена системы и последующие расходы на ее обслуживание. Не каждая организация может себе позволить приобрести дорогостоящие биометрические считыватели и считыватели для смарт-карт, а также тратить средства на их последующее обслуживание. Оптимальным вариантом является построение двух- или трехфакторной процедуры аутентификации в зависимости от необходимого уровня защиты.

Библиографический список

1. *Чернокнижный Г.М.*, *Боховко А.Г.* Подход к разработке комплексной процедуры аутентификации пользователей информационных систем // Сборник научных работ IV Международной научной конференции Евразийского Научного Объединения (г. Москва, апрель 2015). – М.: ЕНО, 2015. – С. 56-57.
2. *Евтеев Дм.*, эксперт по информационной безопасности. Анализ проблем парольной защиты в российских компаниях // Positive Technologies [Электронный ресурс]. – URL: http://www.ptsecurity.ru/ download/PT-Metrics-Passwords-2013.pdf (дата обращения 12.09.2015).
3. *Klein D.V.* Foiling the cracker: A survey of and improvements to, password security. In UNIX Security II: USENIX Workshop Proceedings, Berkeley, CA, 1990 [Электронный ресурс]. – URL: http://www.klein.com/dvk/ publications/passwd.pdf (дата обращения 12.09.2015).
4. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си // Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с.
5. *Комарова Н.*, *Калемберг Д.* Аутентификация в банках: парадокс небезопасности // Аладдин Р.Д. [Электронный ресурс]. – URL: http://www.aladdin-rd.ru/company/pressroom/articles/26159/?sphrase_id= 544374 (дата обращения 12.09.2015).
6. Профессиональное оборудование для контроля доступа и учета рабочего времени // Smartec [Электронный ресурс]. – URL: http://www.smartec-security.ru/ docs/2015_web.pdf (дата обращения 12.09.2015).
7. Решения на основе платформы iCLASSE SE // HID Global [Электронный ресурс]. – URL: http://www.hidglobal.ru/products/readers/ iclass-se (дата обращения 12.09.2015).

1.2. Исследование механизмов изменения контекста выполнения в SQL Server для противодействия нарушению конфиденциальности данных

В системах управления базами данных реализована субъектно-объектная модель безопасности, в которой, как известно, определяются два основополагающих принципа безопасности функционирования:

- идентификация (персонализация) и аутентификация (подтверждение подлинности) всех субъектов и их процессов по отношению к объектам;
- разграничение полномочий субъектов по отношению к объектам и обязательная проверка полномочий любых процессов над данными.

Модель безопасности СУБД SQL Server многоуровневая и должна обеспечивать защиту как на уровне ОС, так и на уровне самого SQL Server и любой базы данных (рис. 1.4).

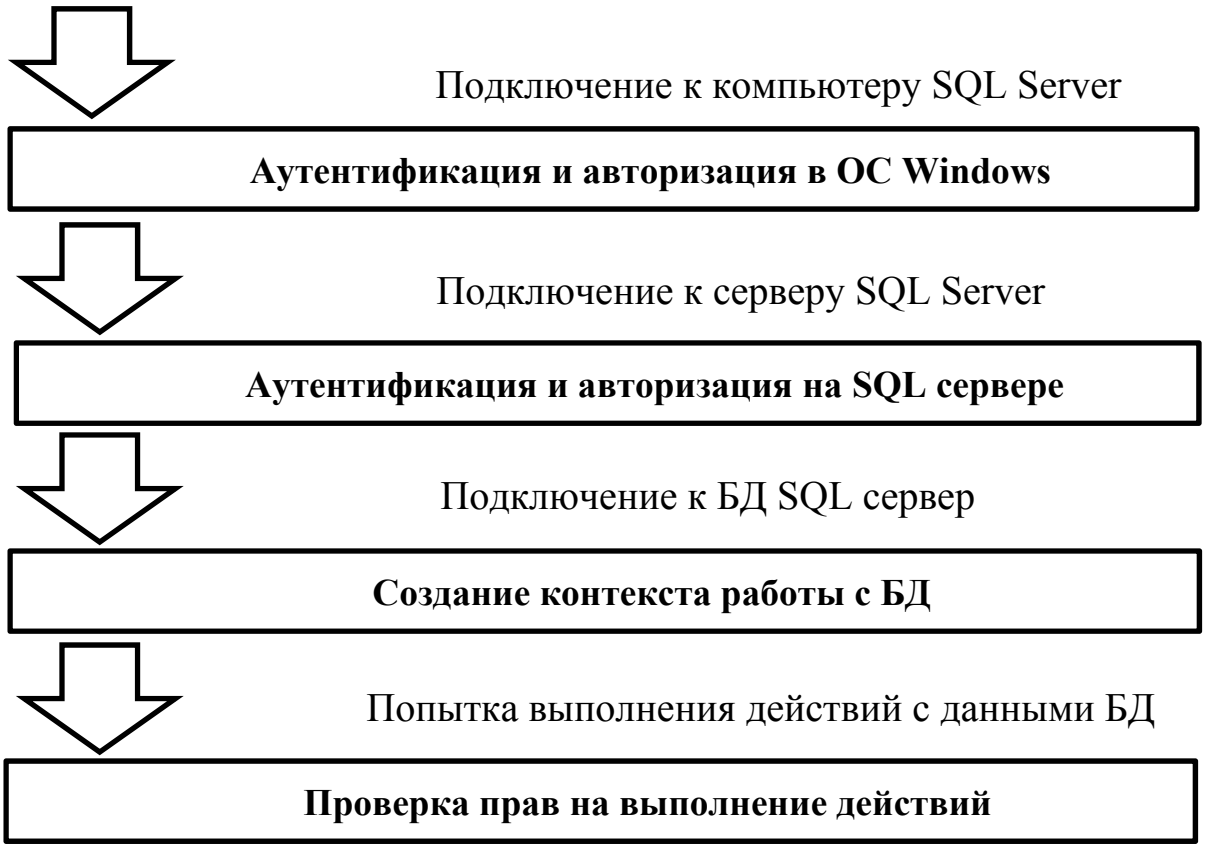


Рис. 1.4. Модель безопасности SQL Server

Соответственно на каждом из этих уровней должна быть реализована своя подсистема безопасности данных. Пользователь должен пройти процедуру обязательной идентификации/аутентификации с последующей авторизацией как на уровне ОС, так и на уровне SQL Server.

В системе безопасности SQL Server применяются понятия «участник безопасности» и «защищаемый объект».

Участники безопасности (субъекты доступа) – это отдельные пользователи, группы и процессы, которым предоставляется доступ к ресурсам SQL Server.

Защищаемые объекты – это сервер, база данных и объекты базы данных.

В модели безопасности SQL Server участники иерархически упорядочены. Область влияния участника зависит от области его определения: Windows, сервер, база данных, – а также от того, коллективный это участник или индивидуальный.

К субъектам доступа уровня операционной системы относится учетная запись пользователя, которая может быть ассоциирована с учетной записью пользователя операционной системы (локальным именем входа Windows или именем входа домена Windows).

Участниками безопасности уровня сервера являются имя входа и серверные роли.

Имя входа – это учетная запись, которая используется для идентификации пользователя при подключении к SQL Server. Информация об именах входа хранится в системном каталоге SQL сервера.

Права доступа учетной записью могут быть получены членством в серверных ролях. Серверные роли предоставляют доступ к операциям и задачам сервера. Роли сервера не зависят от конкретных баз данных.

Каждый из участников имеет идентификатор (ID) и идентификатор безопасности (SID).

При создании учетной записи SQL Server ей назначается идентификатор (principal_id), который определяет учетную запись как защищаемый объект в рамках сервера. Идентификатор безопасности учетной записи SID определяет контекст безопасности учетной записи и является уникальным в пределах экземпляра сервера.

Сведения обо всех участниках безопасности уровня сервера доступны через представление sys.server_principals.

Подключение к серверу не дает автоматического доступа к базам данных. В каждой базе данных, к объектам которой требуется получить доступ, учетная запись пользователя (имя входа) должна ассоциироваться с пользователем (user) базы данных. На основе прав, выданных пользователю базы данных, его учетная запись получает доступ к соответствующей базе данных и ее объектам. Таким образом, с помощью учетной записи пользователя осуществляется подключение к SQL-серверу, после чего определяются его уровни доступа для каждой базы данных в отдельности.

Пользователь базы данных является участником безопасности уровня базы данных. Кроме пользователя на уровне базы данных участниками безопасности являются роль базы данных и роль приложения.

Роль уровня базы данных позволяет назначить права для работы с конкретной базой данных отдельному пользователю или группе. Членом роли может быть другая роль, так что учетным записям можно назначить иерархическую группу прав доступа. В SQL Server существует три типа ролей БД:

- предопределенные роли;
- определяемые пользователем роли;
- роли приложения.

Предопределенными являются встроенные роли, разрешения которых изменить нельзя. С помощью предопределенных ролей можно легко и просто передавать обязанности пользователям.

Определяемые пользователем роли позволяют создавать уникальные наборы разрешений. Самое распространенное назначение пользовательской роли – логически сгруппировать пользователей в соответствии с их правами доступа.

Роль приложения предназначена для работы с приложениями. Роли приложений можно использовать для разрешения доступа к определенным данным только тем пользователям, которые подключены посредством конкретного приложения.

Так же как и для имени входа, при создании пользователя базы данных ему назначается идентификатор (principal_id) и идентификатор безопасности (SID). Идентификатор определяет пользователя как защищаемый объект в рамках базы данных. Идентификатор безопасности, присвоенный пользователю базы данных, является уникальным в рамках этой базы данных и определяет контекст безопасности.

Сведения обо всех участниках безопасности уровня базы данных доступны через представление sys.database_principals.

Для каждого подключения пользователя или имени входа определяется контекст выполнения.

Контекст выполнения представляется парой токенов безопасности: имени входа и пользователя. Токены идентифицируют участников, для которых проверяются разрешения, а также средство, использующееся для проверки подлинности токенов.

Средство проверки подлинности **–** это объект, выполняющий проверку подлинности отдельного участника, т. е. подтверждающий его подлинность. ***Средствами проверки подлинности могут быть*** участники, сертификаты или асимметричные ключи, которые подтверждают подлинность токена. Часто средством проверки подлинности токена является сам экземпляр SQL Server.

Токен безопасности для пользователя и имени входа содержит:

- одного участника сервера или базы данных в качестве первичного идентификатора;
- одного или более участников в качестве вторичных идентификаторов;
- ноль или более средств проверки подлинности;
- права и разрешения первичного и вторичного идентификаторов.

Токен имени входа действителен в пределах экземпляра SQL Server и содержит идентификаторы, для которых проверяются разрешения, связанные с ними на уровне сервера и на уровне базы данных. Первичным идентификатором токена является имя входа. Вторичный идентификатор включает разрешения, унаследованные от серверных ролей и групп.

Токен пользователя действителен только в пределах конкретной базы данных и содержит идентификаторы, для которых проверяются разрешения, связанные с ними на уровне базы данных. Первичным идентификатором является имя пользователя базы данных, а вторичный идентификатор содержит разрешения, унаследованные от ролей базы данных. Идентификаторы токенов пользователя не могут получать разрешения уровня сервера.

Таким образом, контекст выполнения устанавливает идентификатор пользователя или имени входа, чьи разрешения на выполнение инструкций или совершение действий проверяются.

Получить информацию токена имени входа и токена пользователя в сеансе пользователя можно с помощью представлений sys.login_token и sys.user_token, соответственно.

Представление sys.login_token возвращает по одной строке для каждого участника сервера, являющегося частью токена имени входа.

Кроме principal_id, sid и имени участника представление позволяет получить:

- описание типа участника (type). Все типы сопоставляются с sid и могут иметь значения: SQL LOGIN, WINDOWS LOGIN, WINDOWS GROUP, SERVER ROLE, LOGIN MAPPED TO CERTIFICATE, LOGIN MAPPED TO ASYMMETRIC KEY, CERTIFICATE, ASYMMETRIC KEY;

- характеристику (Usage), указывающую на то, как задействован участник безопасности в процессе определения разрешений (GRANT и DENY или DENY ONLY) или он исполняет роль средства проверки подлинности (AUTHENTICATOR).

Представление sys.user_token возвращает по одной строке на каждого участника базы данных, который входит в токен пользователя. В строку выводится идентификатор участника (principal_id) и его идентификатор безопасности (sid), имя участника (Name) и его тип. Тип сопоставляется с sid и может иметь одно из следующих значений SQL USER, WINDOWS

LOGIN, WINDOWS GROUP, ROLE, USER MAPPED TO CERTIFICATE, USE MAPPED TO ASYMMETRIC KEY, CERTIFICATE, ASYMMETRIC KEY. Характеристика Usage имеет те же значения, что и у идентификатора токена имени входа.

Для получения информации токенов имени входа и пользователя базы данных создадим на сервере новое имя входа и предоставим ему разрешение на создание базы данных. Затем в сеансе созданного пользователя создадим базу данных.

С помощью следующего запроса в сеансе администратора создаем на сервере имя входа, соответствующее имени входа домена Windows – AD\ntstud01:

```
CREATE LOGIN [AD\ntstud01] FROM WINDOWS WITH DE-
FAULT_DATABASE=[master], DEFAULT_LANGUAGE=[русский]
```

С помощью системной процедуры включаем имя входа в члены роли, предоставляющей разрешение создания базы данных:

```
exec sp_addsrvrolemember 'ad\ntstud01', dbcreator
GO
```

Предоставим имени входа разрешения членством еще в нескольких серверных ролях:

```
exec sp_addsrvrolemember 'ad\ntstud01', securityadmin
GO
exec sp_addsrvrolemember 'ad\ntstud01', bulkadmin
GO
```

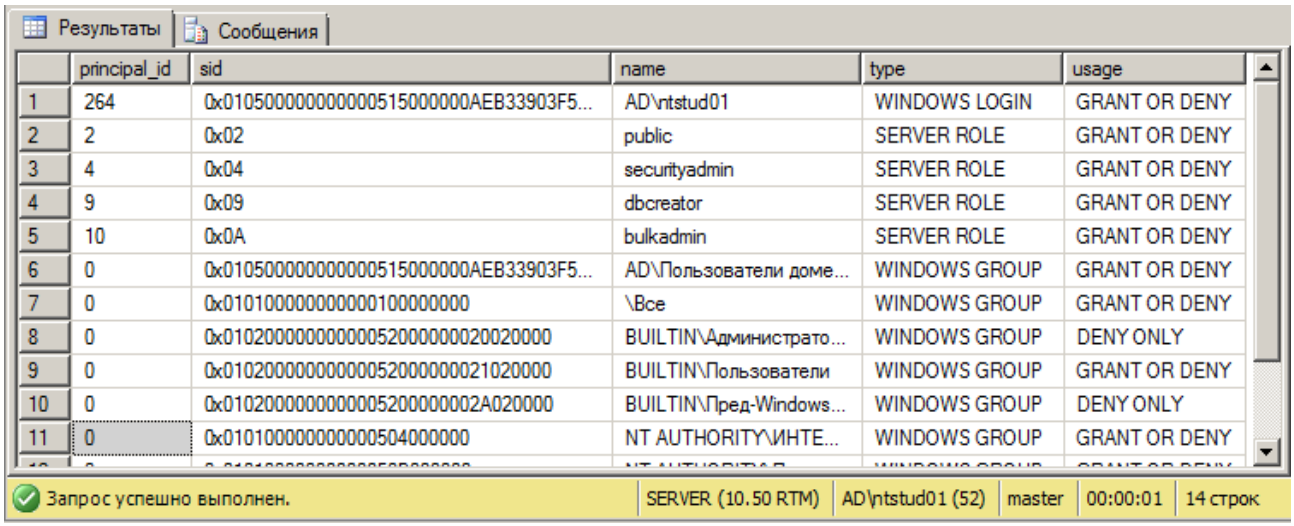
В сеансе имени входа AD\ntstud01 создаем базу данных:

```
USE [master]
GO
CREATE DATABASE [StudDB10]
GO
```

С помощью представления sys.login_token получаем информацию о токене имени входа AD\ntstud01:

```
Use master
go
select * from sys.login_token;
```

Из результирующего набора (рис. 1.5) видно, что учетная запись AD\ntstud01 является первичным идентификатором токена имени входа. Идентификатор principal_id, созданный вместе с ее учетной записью, используется как первичный идентификатор principal_id токена имени входа. Дальше в качестве вторичных идентификаторов указаны роль public и те роли, членом которых AD\ntstud01 является. В качестве вторичных идентификаторов указаны и группы Windows, в которые входит учетная запись AD\ntstud01. Для каждого идентификатора токена указывается, как он задействован в процессе определения разрешений: GRANT и DENY.


Результаты | Сообщения

	principal_id	sid	name	type	usage
1	264	0x0105000000000005150000000AEB33903F5...	AD\ntstud01	WINDOWS LOGIN	GRANT OR DENY
2	2	0x02	public	SERVER ROLE	GRANT OR DENY
3	4	0x04	securityadmin	SERVER ROLE	GRANT OR DENY
4	9	0x09	dbcreator	SERVER ROLE	GRANT OR DENY
5	10	0x0A	bulkadmin	SERVER ROLE	GRANT OR DENY
6	0	0x0105000000000005150000000AEB33903F5...	AD\Пользователи доме...	WINDOWS GROUP	GRANT OR DENY
7	0	0x0101000000000000100000000	\Все	WINDOWS GROUP	GRANT OR DENY
8	0	0x0102000000000005200000020020000	BUILTIN\Администрато...	WINDOWS GROUP	DENY ONLY
9	0	0x0102000000000005200000021020000	BUILTIN\Пользователи	WINDOWS GROUP	GRANT OR DENY
10	0	0x0102000000000005200000002A020000	BUILTIN\Пред-Windows...	WINDOWS GROUP	DENY ONLY
11	0	0x0101000000000000504000000	NT AUTHORITY\ИНТЕ...	WINDOWS GROUP	GRANT OR DENY

Запрос успешно выполнен. | SERVER (10.50 RTM) | AD\ntstud01 (52) | master | 00:00:01 | 14 строк

Рис. 1.5. Токен имени входа, определяющий контекст выполнения для имени входа AD\ntstud01

Что касается роли public, то все пользователи по умолчанию становятся ее членами. Эта роль дает пользователям возможность:

- просматривать системные таблицы и использовать некоторые системные процедуры для просмотра информации базы данных master;
- выполнять операторы, для которых не требуется разрешений.

Анализ информации токена имени входа позволяет выявить администратору безопасности, правильно ли определена политика безопасности пользователя на сервере и нет ли превышения полномочий пользователя членством в серверных ролях или в группах Windows.

У пользователя с именем входа AD\ntstud01 есть по одному токену пользователя для тех баз данных, к которым у него есть доступ. С помощью следующего запроса получим данные токена пользователя с именем входа AD\ntstud01в базе данных master:

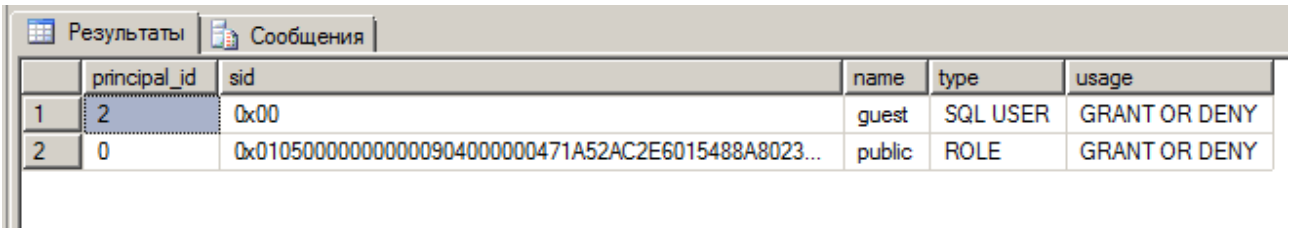
```
use master
go
select * from sys.user_token
```

В полученном по запросу результирующем наборе (рис. 1.6) первичный идентификатор токена пользователя AD\ntstud01 – пользователь guest. Это означает, что AD\ntstud01 – неявный пользователь базы данных master, и имеет к ней доступ по учетной записи guest. Роль public указана как вторичный идентификатор. Токен пользователя AD\ntstud01 в базе данных master содержит все права и разрешения уровня базы данных, принадлежащие пользователю guest и роли public.

Пользователь guest по умолчанию создается при создании новой базы данных. Все имена входа, для которых в базе данных нет учетной записи, получают разрешения, предоставленные пользователю guest.

Пользователя guest нельзя удалить. Чтобы исключить возможность нежелательного подключения к базе данных с помощью guest, нужно отключить этого пользователя, отменив его разрешение на подключение CONNECT с помощью инструкции:

```
REVOKE CONNECT FROM GUEST
```



Результаты | Сообщения

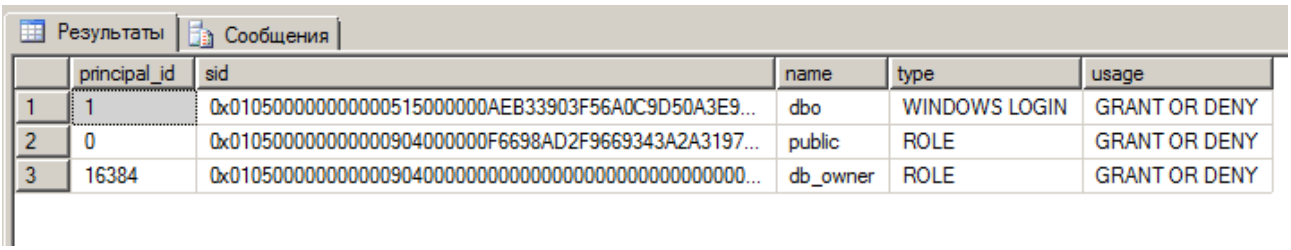
	principal_id	sid	name	type	usage
1	2	0x00	guest	SQL USER	GRANT OR DENY
2	0	0x0105000000000009040000000471A52AC2E6015488A8023...	public	ROLE	GRANT OR DENY

Рис. 1.6. Токен пользователя, определяющий контекст выполнения для имени входа AD\ntstud01 в базе данных master

Следующий запрос позволяет получить данные о токене пользователя в базе данных StudDB01:

```
use StudDB01
go
select * from sys.user_token
```

Первичный идентификатор токена пользователя – пользователь dbo (рис. 1.7). С этим именем связана учетная запись пользователя AD\ntstud01, создавшего базу данных. Пользователю dbo неявно предоставляются все разрешения для работы с базой данных, а также право предоставлять эти разрешения другим пользователям.



Результаты | Сообщения

	principal_id	sid	name	type	usage
1	1	0x0105000000000005150000000AEB33903F56A0C9D50A3E9...	dbo	WINDOWS LOGIN	GRANT OR DENY
2	0	0x0105000000000009040000000F6698AD2F9669343A2A3197...	public	ROLE	GRANT OR DENY
3	16384	0x0105000000000009040000000000000000000000000000000...	db_owner	ROLE	GRANT OR DENY

Рис. 1.7. Токен пользователя, определяющий контекст выполнения для имени входа в базе данных StudDB01

Вторичные идентификаторы токена пользователя роли public и db_owner. Роль db_owner определяет полный доступ ко всем объектам базы данных. Таким образом, контекст выполнения для пользователя AD\ntstud01, определяемый его токеном в базе данных StudDB01, – полный доступ ко всем ее объектам.

По умолчанию сеанс работы пользователя на сервере запускается при входе пользователя в систему и завершается при выходе пользователя

из нее. Во время сеанса все действия подлежат проверке на наличие у пользователя соответствующих разрешений в соответствии с установленным контекстом выполнения. В SQL Server реализован механизм, позволяющий в сеансе подключения к серверу или к базе данных изменять для пользователя контекст выполнения с помощью инструкции EXECUTE AS.

Инструкция EXECUTE AS выполняет явное переключение контекста на контекст выполнения другого пользователя. После переключения контекста проверяются разрешения у имени входа и пользователя этой учетной записи, и происходит его олицетворение.

Если контекст выполнения находится на уровне сервера, то область олицетворения будет следующей:

- учетная запись аутентифицирована на SQL сервере и действительна на этом экземпляре;
- соблюдаются разрешения уровня сервера и принадлежность имени входа к ролям.

Если контекст выполнения находится на уровне базы данных, то область олицетворения будет следующей:

- подлинность маркера имени пользователя для имени пользователя проверена экземпляром SQL Server и действительна для текущей базы данных;
- соблюдаются разрешения уровня базы данных и принадлежность имени пользователя к ролям текущей базы данных. Разрешения уровня серверов, выданные явно для идентификатора маркера пользователя или наследуемые от роли, не соблюдаются.

Олицетворение остается в силе до тех пор, пока не произойдет одно из следующих событий:

- завершится сеанс подключения;
- контекст переключится на другое имя входа или на другого пользователя;
- контекст восстановится до предыдущего контекста выполнения.

Для переключения контекста выполнения на уровне сервера используется инструкция

```
EXECUTE AS LOGIN = 'имя_входа'
```

Указанное в запросе имя входа должно быть зарегистрировано на SQL-сервере.

Для того чтобы пользователь явно мог переключать контекст на уровне сервера с помощью инструкции EXECUTE AS LOGIN, обязательно наличие у него разрешения IMPERSONATE на олицетворение на уровне сервера. Разрешение IMPERSONATE выдается с помощью команды GRANT. Это разрешение позволяет участнику, вызвавшему инструкцию EXECUTE AS LOGIN, олицетворять указанное имя входа в пределах всего экземпляра SQL Server. Всеми разрешениями области уровня сервера владе-

ет sysadmin. При олицетворении имени входа Sysadmin или сам экземпляр SQL Server выступают средствами проверки подлинности уровня сервера.

После смены контекста становится доступен любой ресурс внутри сервера, к которому имеет доступ олицетворенное имя входа учетной записи.

Для переключения контекста выполнения на уровне базы данных используется инструкция

```
EXECUTE AS USER = 'имя_пользователя'
```

Указанное в запросе имя пользователя должно существовать в базе данных. Для того чтобы пользователь явно мог переключать контекст на уровне базы, необходимо наличие разрешения IMPERSONATE на олицетворение внутри области базы данных. Область по умолчанию разрешений IMPERSONATE для пользователей – это сама база данных, владельцем которой является dbo. Владелец базы данных является средством проверки подлинности этих олицетворений. Именно он устанавливает подлинность олицетворенного пользователя и подтверждает его подлинность. Область олицетворения после переключения контекста выполнения ограничена текущей базой данных и контекстом выполнения указанного в инструкции пользователя.

В инструкции EXECUTE AS определен параметр NO REVERT, который указывает, что после переключения контекста вернуться к предыдущему контексту нельзя.

Для возврата к предыдущему контексту используется инструкция REVERT. Вызывающий инструкцию REVERT должен находиться в базе данных, где произошло олицетворение.

Пример. Исследование переключения контекста выполнения с помощью инструкций EXECUTE AS и REVERT.

В учебной базе данных создаем двух пользователей, подключающихся к серверу с именами входа SQL Server.

Создаем имена входа:

```
CREATE LOGIN login1 WITH PASSWORD = 'passw1';
CREATE LOGIN login2 WITH PASSWORD = 'passw2';
GO
В учебной базе данных создаем пользователей:
USE StudDB01;
GO
CREATE USER userDB1 FOR LOGIN login1;
CREATE USER userDB2 FOR LOGIN login2;
GO
```

С помощью функции определяем имя пользователя, контекст выполнения которого установлен в текущем соединении с сервером, и используем функцию ORIGINAL_LOGIN, чтобы узнать имя входа, которое подключилось к экземпляру SQL Server (табл. 1.1).

```
SELECT ORIGINAL_LOGIN() as 'Сеанс',CURRENT_USER AS
'Текущий пользователь';
GO
```

Таблица 1.1

Результат запроса для определения имени входа

Сеанс	Текущий пользователь
AD\Администратор	Dbo

Чтобы user1 мог успешно установить контекст выполнения user2, необходимо user1 выдать разрешение IMPERSONATE олицетворять user2:

```
GRANT IMPERSONATE ON USER:: userDB2 TO userDB1;
GO
```

Переключаем контекст выполнения и определяем имя пользователя, контекст выполнения которого является текущим (табл. 1.2):

```
EXECUTE AS user = 'userDB1';
SELECT ORIGINAL_LOGIN() as 'Сеанс',CURRENT_USER AS
'Текущий пользователь';
GO
```

Таблица 1.2

Результат запроса для контекста login1

Сеанс	Текущий пользователь
AD\Администратор	userDB1

Контекст выполнения установлен для login1.

Находясь в контексте login1, устанавливаем контекст выполнения для login2 (табл. 1.3).

```
EXECUTE AS USER = 'userDB2';
SELECT ORIGINAL_LOGIN() as 'Сеанс',CURRENT_USER AS
'Текущий пользователь';
GO
```

Таблица 1.3

Результат запроса: для контекста login2

Сеанс	Текущий пользователь
AD\Администратор	userDB2

Контекст выполнения для login2 установлен.

Для перехода на предыдущий контекст выполнения выполняем инструкцию

```
REVERT;
```

Отображаем текущий контекст выполнения (табл. 1.4).

```
SELECT ORIGINAL_LOGIN() as 'Сеанс',CURRENT_USER AS
'Текущий пользователь';
GO
```

Таблица 1.4

Результат запроса для возврата к предыдущему контексту

Сеанс	Текущий пользователь
AD\Администратор	userDB1

Установлен контекст выполнения для login1.

Для возвращения в контекст пользователя DBO повторно выполняет

```
REVERT;
```

И смотрим его имя (табл. 1.5):

```
SELECT ORIGINAL_LOGIN() as 'Сеанс',CURRENT_USER AS
'Текущий пользователь';
```

Таблица 1.5

Результат запроса для возврата к исходному контексту

Сеанс	Текущий пользователь
AD\Администратор	Dbo

Контекст выполнения может определяться не только пользователем, выполнившим соединение с сервером, но и выполняющимся модулем. Пользователь, модуль которого выполняет олицетворение, должен обладать разрешениями на все объекты, с которыми работает модуль. Однако не всегда пользователю, которому предоставляются разрешения на выполнение модуля, должны предоставляться явные разрешения на те объекты, на которые ссылается модуль.

В SQL server модуль может выполняться в контексте вызывающего пользователя, в контексте владельца модуля или в контексте любого указанного пользователя. Для определения контекста выполнения пользовательских модулей: функций, процедур, запросов и триггеров, – в описании модуля используется параметр EXECUTE AS.

Синтаксис команды создания процедуры с указанием контекста выполнения.

```
CREATE PROC имя
```

```
WITH EXECUDE AS {CALLER|имя_пользователя|SEFT|OWNER
}
As
<инструкции SQL>
```

Определяя с помощью параметра EXECUDE AS контекст, в котором должен выполняться модуль, можно управлять тем, какая пользовательская учетная запись SQL Server используется для проверки разрешений модуля на объекты базы данных.

EXECUDE AS CALLER указывает, что инструкция выполняется в контексте вызывающего процедуру пользователя. Пользователь должен иметь разрешение на выполнение процедуры и все необходимые разрешения на объекты, с которыми работает модуль.

EXECUTE AS имя_пользователя указывает, что инструкции внутри модуля выполняются в контексте указанного пользователя. Этот пользователь должен иметь все необходимые разрешения на объекты, с которыми работает процедура. Следует помнить, что пользователя, в контексте которого выполняется модуль, нельзя удалить до тех пор, пока модуль не сменит контекст выполнения.

EXECUDE AS SEFT означает, что инструкция выполняется в контексте пользователя, создавшего или изменившего модуль.

Предложение EXECUTE AS OWNER указывает, что операторы внутри модуля вызываются в контексте владельца модуля. Если у модуля нет владельца, им становится владелец схемы модуля. Это удобно в том случае, если нужно иметь возможность изменить владельца модуля без внесения изменений в его код. В этом случае параметр OWNER автоматически сопоставляется с текущим владельцем модуля во время выполнения.

Переключение контекста выполнения с помощью EXECUTE AS LOGIN или EXECUTE AS USER позволяет изменять область олицетворения на уровне сервера или на уровне базы данных. Контекст выполнения, принадлежащий владельцу области как ее средству проверки подлинности, действителен внутри всей этой области. Это обусловлено тем, что владелец области, например базы данных, является неявно доверенным для всех сущностей внутри базы данных.

В SQL Server реализована возможность выборочного расширения текущей области олицетворения базы данных путем настройки доверительной модели отношений между двумя базами данных.

Область олицетворения контекста, установленного внутри базы данных, можно расширить на другие базы данных, если выполняются следующие условия:

- средство проверки подлинности (владелец базы данных, сертификат или асимметричный ключ), с помощью которого подписан

модуль, должно быть доверенным в целевой области (другой базе данных);

- если средством проверки подлинности является владелец базы данных, то база данных – источник должна быть помечена как заслуживающая доверия.

Доверие средству проверки подлинности (SQL Server) устанавливается путем выдачи средству проверки подлинности разрешения AUTHENTICATE, если целевая область является другой базой данных.

Доверие базе данных и ее содержимому устанавливается с помощью свойства базы данных TRUSTWORTHY. Для этого этому свойству следует присвоить значение ON. Значение свойству TRUSTWORTHY в базе данных могут задавать только члены предопределенной серверной роли sysadmin. По умолчанию подключенные базы данных не помечаются как заслуживающие доверия.

После того как владелец базы данных стал доверенным для внешнего ресурса и сама база данных заслуживает доверие, любой олицетворенный контекст, установленный в этой базе данных, действителен во всей целевой области, которая доверяет владельцу базы данных.

Если база данных является доверенной не целиком и необходимо доверять только небольшому числу модулей в базе данных и при этом доступ к ресурсам внешней базы данных осуществляется с помощью предложения EXECUTE AS в модуле, то в качестве средства проверки подлинности используются сертификаты или асимметричные ключи. В этом случае модуль в базе данных должен содержать электронную подпись.

Электронная подпись модуля удостоверяет, что код внутри модуля может изменять только пользователь с доступом к закрытому ключу, с помощью которого подписан этот модуль. Учитывая гарантии, обеспечиваемые процессом подписи, можно доверять сертификату или асимметричному ключу, указанному в подписи. Таким образом, доверять можно не только владельцу базы данных, но и владельцу сертификата или асимметричного ключа.

Подписанный модуль становится доверенным после выдачи разрешения AUTHENTICATE пользователю во внешней базе данных, сопоставленному с сертификатом или асимметричным ключом. После этого контекст выполнения, установленный внутри модуля, подписанного с помощью доверенного сертификата, действителен в целевой области, в которой является доверенным этот сертификат.

Рассмотрим на конкретном примере расширение текущей области олицетворения базы данных путем настройки доверительной модели отношений между двумя базами данных.

Условие задания: В тестовой базе данных testdb1 в сеансе владельца базы данных login1 создать хранимую процедуру p1, которая запрашивает

данные таблиц t1 и t2. Вторая таблица находится в базе данных testdb2. Необходимо обеспечить расширение области олицетворения, чтобы реализовать межбазовую цепочку владения объектами, к которым обращается процедура при выполнении. Для этого следует установить первую базу данных TRUSTWORTHY и предоставить ее владельцу (login1) разрешение AUTHENTICATE во второй базе данных. Создать в базе данных testdb1 пользователя и предоставить ему разрешение на выполнение процедуры. В процедуре неявно переключать контекст выполнения хранимой процедуры с вызвавшего пользователя на владельца процедуры с помощью EXECUTE AS.

Создаем две базы данных testdb1 и testdb2.

```
IF EXISTS (SELECT * FROM sys.databases WHERE [name] =
'testdb1')
DROP DATABASE testdb11;
GO
CREATE DATABASE testdb1;
GO
IF EXISTS (SELECT * FROM sys.databases WHERE [name] = '
testdb2')
DROP DATABASE testdb2;
GO
CREATE DATABASE testdb2;
GO
```

Создаем имена входа login1 и login2.

```
USE master;
GO
CREATE LOGIN login1 WITH PASSWORD = 'Password_login1',
CHECK_POLICY =OFF;
GO
CREATE LOGIN login2 WITH PASSWORD = 'Password_login2',
CHECK_POLICY =OFF;
GO
```

Меняем владельцев базы данных, передавая их не административным учетным записям login1 и login2 .

```
ALTER AUTHORIZATION ON DATABASE:: testdb1 TO login1;
GO
ALTER AUTHORIZATION ON DATABASE:: testdb2 TO login2;
GO
```

В базе данных testdb2 создаем и заполняем данными таблицу t2.

```
USE testdb2;
CREATE TABLE t2 (c3 char(20) not null, c4 int not null,);
GO
```

```
Insert into t2 values(’Петров’, 1),(‘Иванов’,1),(‘Соловьев’,3)
GO
```

В testdb1 создаем и заполняем данными таблицу t1 и затем создаем хранимую процедуру.

```
USE testdb1;
GO
CREATE TABLE t1(c1 int NOT NULL, c2 char(20) NOT NULL)
GO
Insert into t1 values(1,’ВМ’),(2,’ТВ’),(3,’ЗБД’),(4,’ООП’)
GO
create procedure p1
with execute as owner
as
begin
select c1,c2,a.c3,a.c4
from t1 inner join testdb2.dbo.t2 a on t1.c1=a.c4
end
```

Создаем пользователя proc_user, которому предоставим разрешение на выполнение процедуры p1.

```
USE master;
CREATE LOGIN proc_user WITH PASSWORD = 'P@ssword_p1',
CHECK_POLICY =OFF;
GO
USE testdb1;
CREATE USER proc_user FOR LOGIN proc_user;
GO
GRANT EXEC ON p1 TO proc_user;
GO
```

Переключаем контекст выполнения на пользователя proc_user и просматриваем информацию его токена (рис. 1.8).

```
USE testdb1;
EXECUTE AS USER = ' proc_user ';
GO
SELECT * FROM sys.user_token;
GO
```

Результаты | Сообщения

	principal_id	sid	name	type	usage
1	5	0x4395E06CC760B646BDE8EC21A365D28A	proc_user	SQL USER	GRANT OR DENY
2	0	0x010500000000000904000000083741B006749C04BA943C0...	public	ROLE	GRANT OR DENY

Рис. 1.8. Токен пользователя proc_user в базе данных testdb1

Выполняем хранимую процедуру в контексте пользователя proc_user

```
EXEC p1;
GO
```

Получаем сообщение:

```
Сообщение 916, уровень 14, состояние 1, процедура p1, стро-
ка 5
Серверу-участнику "login1" не удалось обратиться к базе дан-
ных "testdb2" в текущем контексте безопасности.
Сообщение 263, уровень 16, состояние 1, строка 1
Необходимо указать таблицу для выбора.
```

Возвращаемся в контекст пользователя DBO.

```
REVERT;
GO
```

Для того чтобы testdb2 доверяла login1, в базе данных testdb2 создаем пользователя из учетных данных login1 и предоставляем ему разрешение AUTHENTICATE

```
USE testdb2;
CREATE USER login1 FOR LOGIN login1;
GO
GRANT AUTHENTICATE TO login1;
execute as user='login1'
```

Просматриваем токен пользователя login1 в testdb2 инструкцией и получаем результат, представленный на рис. 1.9.

```
SELECT * FROM sys.user_token;
GO
```

Результаты | Сообщения

	principal_id	sid	name	type	usage
1	5	0xC493452732F39E428B4EF3621D97FB81	login1	SQL USER	GRANT OR DENY
2	0	0x010500000000000904000000083741B006749C04BA943C0...	public	ROLE	GRANT OR DENY

Рис. 1.9. Токен пользователя login1 в базе данных testdb2

Возвращаемся в контекст dbo:

```
REVERT
GO
```

Устанавливаем базу данных testdb1 заслуживающей доверия, чтобы экземпляр SQL Server доверял этой базе данных и ее содержимому.

```
USE master;
ALTER DATABASE testdb1 SET TRUSTWORTHY ON
```

Пользователю login1 в testdb2 выдаем разрешение select на таблицу t2:

```
USE testdb2;
```

```
GO
GRANT SELECT ON t2 TO login1;
```

Переключаем в базе данных testdb1 контекст выполнения на пользователя proc_user и просматриваем его токен (рис. 1.10), сравнивая с рис. 1.8.

```
USE testdb1;
EXECUTE AS USER = 'proc_user';
GO
SELECT * FROM sys.user_token;
GO
```

Результаты | Сообщения

	principal_id	sid	name	type	usage
1	5	0x4395E06CC760B646BDE8EC21A365D28A	proc_user	SQL USER	GRANT OR DENY
2	0	0x010500000000000904000000083741B006749C04BA943C0...	public	ROLE	GRANT OR DENY
3	1	0xC493452732F39E428B4EF3621D97FB81	dbo	SQL USER	AUTHENTICATOR
4	16384	0x010500000000000904000000000000000000000000000000...	db_owner	ROLE	AUTHENTICATOR

Рис. 1.10. Токен пользователя proc_user в базе данных testdb1 после расширения области олицетворения

Поскольку средству проверки подлинности login1 было предоставлено разрешение AUTHENTICATE в базе данных testdb2, то контекст для пользователя, установленный предложением EXECUTE AS в хранимой процедуре P1 в базе данных testdb1, является доверенным в базе данных testdb2. В токен пользователя базы данных testdb1 в качестве вторичных идентификаторов добавлены средства проверки подлинности, являющиеся идентификаторами токена пользователя login1 в базе данных testdb2.

Выполняем хранимую процедуру в контексте пользователя proc_user:

```
EXEC p1;
GO
```

Получаем результат (рис. 1.11) после успешной авторизации.

Результаты | Сообщения

	c1	c2	c3	c4
1	1	ВМ	Петров	1
2	1	ВМ	Иванов	1
3	3	ЗБД	Соловьев	3

Рис. 1.11. Результат работы процедуры p1

Посмотрим, может ли пользователь извлекать данные из таблицы t1:

```
SELECT * FROM t1;
GO
```

Получаем сообщение:

```
Сообщение 229, уровень 14, состояние 5, строка 1
Запрещено разрешение "SELECT" на объект "t1" базы данных
"testdb1", схемы "dbo".
```

Проверим, может ли пользователь извлекать данные из таблицы t2:

```
SELECT * from testdb2...t2;
GO
```

Получаем сообщение:

```
Сообщение 916, уровень 14, состояние 1, строка 1
Серверу-участнику "proc_user" не удалось обратиться к базе
данных "testdb2" в текущем контексте безопасности.
```

Возвращаемся в базе данных testdb1 к контексту dbo:

```
REVERT;
GO
```

Проверим, может ли пользователь login1 базы данных testdb2 извлекать данные из таблицы t1 testdb1:

```
USE testdb2;
GO
execute as user='login1'
SELECT * FROM testdb1...t1;
GO
```

Получаем сообщение:

```
Сообщение 916, уровень 14, состояние 1, строка 1
Серверу-участнику "login1" не удалось обратиться к базе дан-
ных "testdb1" в текущем контексте безопасности.
```

Проведенные в примере исследования продемонстрировали расширение области олицетворения на внешнюю базу данных для пользователя, в контексте которого выполняется модуль.

Возможность расширения области олицетворения контекста для имени входа, пользователя или выполняющегося модуля, безусловно, является актуальным в системе безопасности, так как позволяет на время осуществлять изменения полномочий пользователя на сервере или в базе данных. Однако любое изменения полномочий, особенно в сторону их расширения, можно рассматривать как потенциальную угрозу нарушения конфиденциальности данных. Знание механизмов изменения контекста выполнения в SQL Server и умение их правильного применения позволит исключить возможность возникновения таких угроз.

Глава 2. МЕТОДЫ АНАЛИЗА ЗАЩИЩЕННОСТИ

2.1. Исследование защищенности корпоративной сети учреждения

Аудит информационной безопасности

Под аудитом информационной безопасности (ИБ) понимается периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению информационной безопасности [1].

Результаты квалифицированно выполненного аудита ИБ организации позволяют построить оптимальную по эффективности и затратам систему обеспечения информационной безопасности (СОИБ), представляющую собой комплекс технических средств, а также процедурных, организационных и правовых мер, объединенных на основе модели управления ИБ.

В результате проведения аудита могут быть получены как качественные (например, перечень уязвимостей в программно-аппаратном обеспечении с их классификацией по трехуровневой шкале опасности), так и количественные (например, цена риска, вероятность риска и т. п.).

Объективность аудита обеспечивается, в частности, тем, что оценка состояния ИБ производится специалистами на основе определенной методики, позволяющей объективно проанализировать все составляющие СОИБ. Аудит ИБ может представлять собой услугу, которую предлагают специализированные фирмы, тем не менее в организации должен проводиться внутренний аудит ИБ, выполняемый, например, администраторами безопасности.

Традиционно выделяют три типа аудита ИБ, которые различаются перечнем анализируемых компонентов СОИБ и получаемыми результатами:

- экспертный аудит;
- аудит на соответствие стандартам ИБ;
- активный аудит.

Экспертный аудит

Экспертный аудит предназначен для оценивания текущего состояния ИБ на нормативно-методологическом, организационно-управленческом и процедурном уровнях. Экспертный аудит проводится преимущественно внешними аудиторами, его выполняют силами специалистов по системному управлению.

В рамках экспертного аудита проводится анализ организационно-распорядительных документов, таких как политика безопасности, план

защиты, положения и инструкции. Организационно-распорядительные документы оцениваются на предмет достаточности и непротиворечивости декларируемым целям и мерам ИБ, а также на предмет соответствия стратегической политике руководства в вопросах ИБ.

Результаты экспертного аудита могут содержать рекомендации по совершенствованию нормативно-методологических, организационно-управленческих и процедурных компонентов СОИБ.

Аудит на соответствие стандартам ИБ

В ряде случаев проводится аудит на соответствие стандартам ИБ. Специально уполномоченные организации-аудиторы по результатам аудита принимают решение и выдают документальное подтверждение о соответствии СОИБ тому или иному эталонному стандарту (проводят сертификацию). Сертификация является показателем качества СОИБ и поднимает престиж и уровень доверия к организации.

Методика проведения инструментальных проверок активного аудита

Инструментальные проверки (ИП) выполняются в процессе активного аудита ИБ. Они состоят из набора заранее согласованных тестов, направленных на получение характеристик об уровне защищенности выбранных ПИБ. Для проведения инструментальных проверок может быть предложена следующая методика, предполагающая тестирование возможности несанкционированного доступа (НСД) к информации, обрабатываемой или хранящейся в АИС, как изнутри организации, так и из внешних сетей. Методика включает три этапа: анализ структуры АИС, внутренний аудит, внешний аудит.

На этапе анализа структуры АИС с позиций ИБ производится анализ и инвентаризация информационных ресурсов и СВТ: формируется перечень защищаемых сведений; описываются информационные потоки, структура и состав АИС; проводится категорирование ресурсов, подлежащих защите.

На втором этапе осуществляется внутренний аудит АИС, включающий анализ настроек АИС с точки зрения ИБ. На данном этапе с учетом известных изъянов ОС и специализированных СЗИ осуществляется анализ защищенности от опасных внутренних воздействий. Исследуется возможность несанкционированных действий легальных пользователей компьютерной сети, которые могут привести к модификации, копированию или разрушению конфиденциальных данных. Анализ осуществляется путем детального изучения настроек безопасности средств защиты с использованием как общеупотребимых (в том числе входящих в арсенал хакеров), так и специально разработанных автоматизированных средств исследования уязвимости АИС. Анализируются следующие компоненты АИС:

- средства защиты ПК – возможность отключения программно- аппаратных систем защиты при физическом доступе к выключенным станциям; использование и надежность встроенных средств парольной защиты BIOS;
- состояние антивирусной защиты – наличие в АИС вредоносных программ, возможность их внедрения через машинные носители, сеть Интернет;
- ОС – наличие требуемых настроек безопасности;
- парольная защита в ОС – возможность получения файлов с зашифрованными паролями и их последующего дешифрования;
- возможность подключения с пустыми паролями, подбора паролей, в том числе по сети;
- система разграничения доступа пользователей АИС к ресурсам – формирование матрицы доступа; анализ дублирования и избыточности в предоставлении прав доступа; определение наиболее осведомленных пользователей и уровней защищенности конкретных ресурсов; оптимальность формирования рабочих групп;
- сетевая инфраструктура – возможность подключения к сетевому оборудованию для получения защищаемой информации путем перехвата и анализа сетевого трафика; настройки сетевых протоколов и служб;
- аудит событий безопасности – настройка и реализация политики аудита;
- прикладное ПО – надежность элементов защиты используемых АРМ; возможные каналы утечки информации; анализ версий используемого программного обеспечения на наличие уязвимых мест;
- СЗИ: надежность и функциональность используемых СЗИ; наличие уязвимых мест в защите; настройка СЗИ.

На третьем этапе осуществляется внешний аудит АИС, оценивающий состояние защищенности информационных ресурсов организации от НСД, осуществляемого из внешних сетей, в том числе из Интернета. Последовательно анализируются следующие возможности проникновения извне:

- получение данных о внутренней структуре АИС – наличие на web-серверах информации конфиденциального характера; выявление настроек DNS- и почтового серверов, позволяющих получить информацию о внутренней структуре АИС;
- выявление компьютеров, подключенных к сети и достижимых из Интернет-сканирования по протоколам ICMP, TCP, UDP; определение степени доступности информации об используемом в АИС ПО и его версиях; выявление активных сетевых служб; определение типа и версии ОС, сетевых приложений и служб;

- получение информации об учетных записях, зарегистрированных в АИС с применением утилит, специфичных для конкретной ОС;
- подключение к доступным сетевым ресурсам – определение наличия доступных сетевых ресурсов и возможности подключения к ним;
- использование известных уязвимостей в программном обеспечении МЭ, выявление неверной конфигурации МЭ;
- выявление версий ОС и сетевых приложений, подверженных атакам типа «отказ в обслуживании»;
- тестирование возможности атак на сетевые приложения – анализ защищенности web-серверов, тестирование стойкости систем удаленного управления, анализ возможности проникновения через имеющиеся модемные соединения.

По результатам тестирования оформляется экспертное заключение, описывающее реальное состояние защищенности АИС от внутренних и внешних угроз, содержащее перечень найденных изъянов в настройках систем безопасности. На основании полученного заключения разрабатываются рекомендации по повышению степени защищенности АИС, по администрированию систем, по применению СЗИ.

Реализация методики требует постоянного обновления знаний об обнаруживаемых изъянах в системах защиты. Не все этапы методики могут быть автоматизированы. Во многих случаях требуется участие эксперта, обладающего соответствующей квалификацией.

На основании анализа методов проведения аудита информационной безопасности следует, что наиболее подходящим для исследования защищенности корпоративной сети является метод инструментальной проверки активного аудита, так как он позволяет получить наиболее подробные данные об уязвимостях корпоративной сети, на основании которых можно составить определенное заключение об уровне защищенности этой сети и предоставить рекомендации для его повышения.

Таким образом, для исследования защищенности сети необходимо выбрать соответствующее требованиям средство инструментальной проверки, в данном случае – сетевой сканер безопасности.

Сравнительный анализ средств сетевого сканирования

Сетевые сканеры безопасности могут быть использованы для различных целей. В случае с исследованием безопасности корпоративной сети наиболее интересны результаты сравнения сетевых сканеров безопасности в ходе проведения тестов на проникновение в отношении узлов сетевого периметра.

При этом оценивается:

- Количество найденных уязвимостей.
- Число ложных срабатываний (False Positives).

- Число пропусков (False Negatives).
- Причины пропусков.
- Полнота базы проверок (в контексте данной задачи).
- Качество механизмов инвентаризации и определения версий ПО.
- Точность работы сканера (в контексте данной задачи).

Для участия в тестовых испытаниях были отобраны сканеры, представленные в табл. 2.1.

Таблица 2.1

Сетевые сканеры безопасности, использованные в ходе сравнения

Название	Версия	Ссылка
Nessus	3.2.1	http://www.nessus.org/download
MaxPatrol	8.0 (Сборка 1178)	http://www.ptsecurity.ru/maxpatrol.asp
Internet Scanner	7.2.58	http://www-935.ibm.com/services/us/index.wss/offering/iss/a1027208
Retina Network Security Scanner	5.10.2.1389	http://www.eeye.com/html/products/retina/index.html
Shadow Security Scanner (SSS)	7.141 (Build 262)	http://www.safety-lab.com/en/products/securityscanner.htm
NetClarity Auditor	6.1	http://netclarity.com/branch-nacwall.html

По результатам определения сервисов и приложений баллы были просуммированы, при этом за ошибочное определение сервиса или приложения вычитался один балл (табл. 2.2). Из табл. 2.2 видно, что наибольшее количество баллов (108) набрал сканер MaxPatrol.

Таблица 2.2

Итоговые результаты по всем объектам сканирования

Показатель	MaxPatrol	Internet Scanner	Retina	Nessus	Shadow Security Scanner	Net Clarity Auditor
Идентификация сервисов и приложений, баллы	108	66	80	98	79	54
Найдено уязвимостей, всего	163	51	38	81	69	57
Из них ложных срабатываний (false positives)	8	3	4	7	36	14
Найдено правильно (из 225 возможных)	155	48	34	74	33	43
Пропуски (false negatives)	70	177	191	151	192	182

Окончание табл. 2.2

Показатель	MaxPatrol	Internet Scanner	Retina	Nessus	Shadow Security Scanner	Net Clarity Auditor
Из них по причине отсутствия в базе	63	170	165	59	150	179
Из них вызванные необходимостью аутентификации	0	6	16	36	0	0
По другим причинам	7	1	10	56	42	3

Далее были проанализированы общее число найденных всеми сканерами уязвимостей и число ложных срабатываний. Наибольшее число уязвимостей было найдено сканером MaxPatrol (см. табл. 2.2).

Всего на всех 16 узлах всеми сканерами было найдено (и впоследствии подтверждено ручной проверкой) 225 уязвимостей. Распределение результатов приведено в табл. 2.2.

В ходе сравнительного анализа были проанализированы причины пропусков уязвимостей и были отделены те, которые были сделаны по причине отсутствия проверок в базе. На рис. 2.1 представлены причины пропусков уязвимостей сканерами.

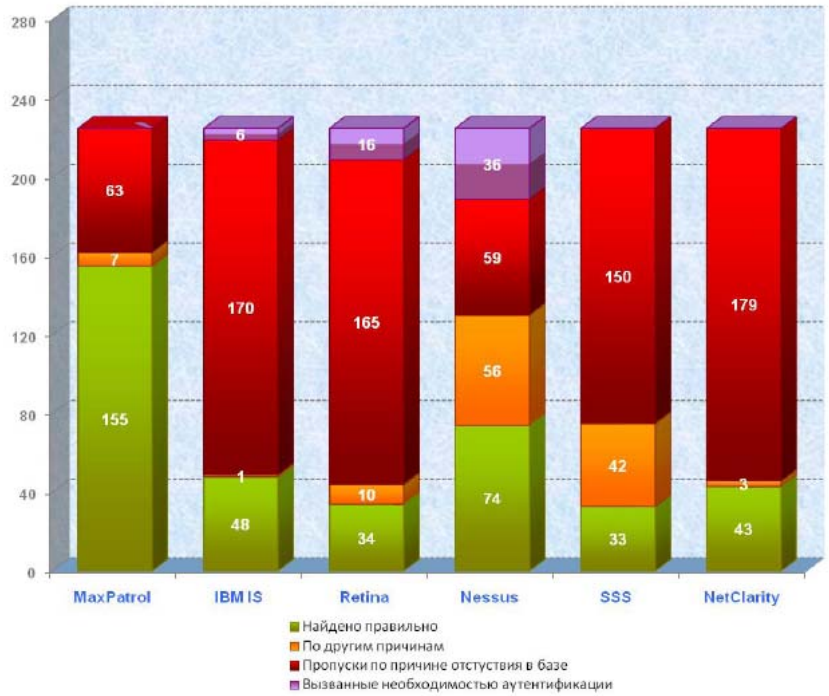


Рис. 2.1. Причины пропусков уязвимостей

На рис. 2.2 представлено отношение числа ложных срабатываний к общему числу найденных уязвимостей, этот показатель в определенном смысле можно назвать точностью работы сканера.

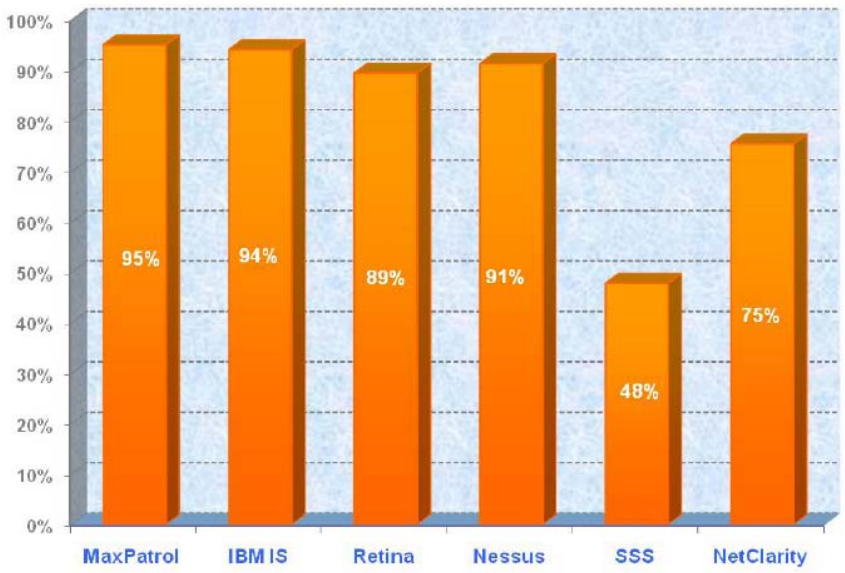


Рис. 2.2. Точность работы сканеров

Из этой диаграммы видно, что наивысшая точность (95%) достигнута сканером MaxPatrol. Хотя число ложных срабатываний у него не самое низкое, такой показатель точности достигнут за счет большого количества найденных уязвимостей.

Еще один расчетный показатель – это полнота базы (рис. 2.3). Он рассчитан как отношение числа уязвимостей, найденных правильно, к общему числу уязвимостей (в данном случае – 225) и характеризует масштабы «пропусков».

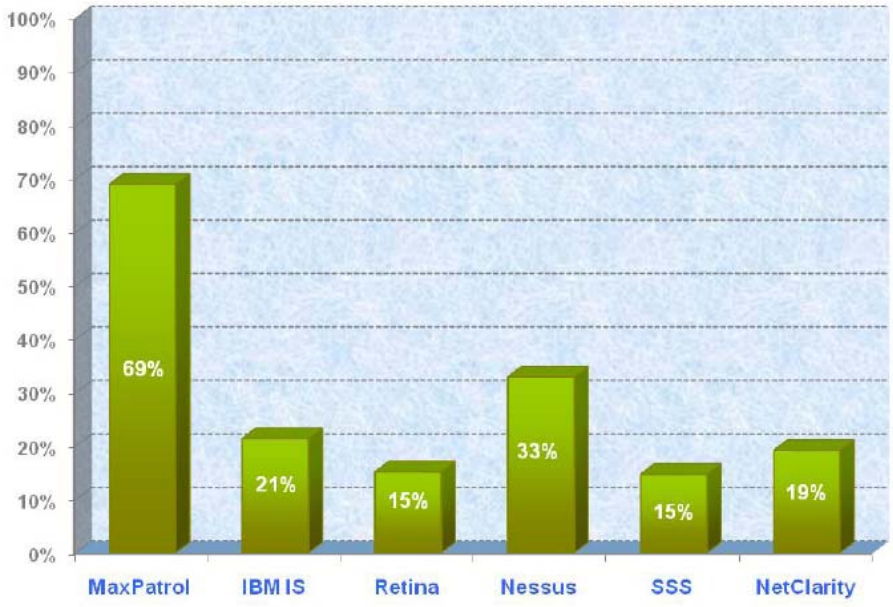


Рис. 2.3. Полнота базы

Аналогичным образом были посчитаны результаты по остальным узлам. После подсчета итогов получилась следующая таблица (см. табл. 2.2).

На основании проведенного анализа был выбран наиболее эффективный сетевой сканер безопасности MaxPatrol (сертификат соответствия ФСТЭК России от 08.07.2013 № 2922) [2].

Таким образом, для исследования защищенности корпоративной сети был выбран частный метод проведения инструментальной проверки активного аудита с использованием рассмотренного нами средства проверки защищенности сети MaxPatrol.

Контроль защищенности корпоративной сети учреждения

Под безопасностью информации автоматизированной системы (АС) понимается состояние защищенности, обрабатываемой в ней информации, при котором обеспечены ее конфиденциальность, доступность и целостность. Наличие уязвимостей может привести к нарушению данных свойств информации.

Под уязвимостью понимается свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

На основании пункта 3.24 руководящего документа [3], с целью своевременного выявления и предотвращения утечки информации, обрабатываемой в АС и ее локально-вычислительной сети (ЛВС), исключения или существенного затруднения несанкционированного доступа к ней и предотвращения специальных программно-технических воздействий, вызывающих нарушение конфиденциальности, целостности и доступности информации, необходимо проводить контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, а в частности, проводить сбор информации об общем уровне защищенности посредством использования инструментального средства анализа уязвимостей.

Также контроль обеспечения безопасности государственной информационной системы в данном случае подразумевает под собой использование инструментальных средств [4], пример которых приведен в табл. 2.3.

Таблица 2.3

Пример инструментальных средств, используемых для обеспечения контроля защищенности корпоративной сети учреждения

Наименование	Количество
Мобильное АРМ на базе ноутбука Lenovo X230	1
Средство анализа защищенности MaxPatrol	1
Операционная система Windows 7	1
Пакет Microsoft Office 2007	1
Средство антивирусной защиты Kaspersky Endpoint Security 10	1

Экспертно-инструментальное обследование объекта информатизации с использованием программного средства MaxPatrol на предмет определения уровня защищенности

При выполнении работ использовался только экспертно-инструментальный (инструментальный) метод проведения обследования. Сканирование узлов сети осуществлялось в автоматизированном режиме сертифицированным по требованиям безопасности информации сканером безопасности путем выполнения проверок в соответствии с предварительно сформированным планом. После окончания проверок производилась регистрация результатов их выполнения.

Также производилась инвентаризация объекта обследования, которая включает в себя поиск и обнаружение компонентов объекта обследования, определение состава сетевых сервисов, состава используемых технических средств и характеристик.

Поиск и обнаружение компонентов объекта обследования производились следующими методами:

1. Метод пассивного прослушивания.
2. Метод активного сканирования.

Поиск и обнаружение компонентов объекта обследования методом пассивного прослушивания выполнялись путем оценки количества функционирующих на объекте обследования устройств, их сетевых адресов, выявленных аномалий (например, использование в одном коммутационном поле сетевых адресов, принадлежащих IP-сетям, не заявленным для проведения обследования) и сопоставления этих данных, с исходными данными, полученными в результате предыдущей инвентаризации.

Получение данных о компонентах объекта обследования осуществлялось с использованием технологических особенностей применяемых протоколов канального и сетевого уровней (применение широковещательных (broadcast) и мультивещательных (multicast) пакетов). В случае если вычислительная сеть, входящая в объект обследования, сегментирована с использованием маршрутизаторов или с использованием технологии виртуальных локальных сетей (VLAN), сбор данных производился в каждом сегменте такой вычислительной сети. Для этого рабочие станции, используемые для проведения инструментального обследования, логически, а при необходимости и физически включались поочередно в состав всех сегментов вычислительной сети.

Поиск и обнаружение компонентов объекта обследования методом активного сканирования выполнялся путем использования сканеров безопасности. Для увеличения вероятности обнаружения узлов сети, на которых производится фильтрация пакетов, поиск производился, ис-

пользуя ARP и ICMP протоколы. Рабочая станция, используемая для проведения инструментального обследования с установленными сканерами безопасности, находилась в одном широковещательном домене вычислительной сети объекта обследования (подсеть VLAN) с проверяемыми узлами сети.

Определение состава сетевых сервисов осуществлялось в целях верификации перечня и версий сервисов (служб), предоставляемых компонентами объекта обследования.

Верификация сервисов производится экспертами Исполнителя в случае, если они:

- не указаны в исходных данных;
- не являются характерными для данного типа узла (например, ftp, http сервер на рабочей станции);
- обладают выявленными в ходе проверки уязвимостями.

По результатам проверки в отчете производится сводная таблица, в которой указываются:

- IP-адрес технического средства;
- аппаратный (mac) адрес сетевого адаптера технического устройства;
- производитель сетевого адаптера (по mac адресу);
- DNS имя технического средства;
- NetBIOS для технического средства;
- операционная система (по результатам совокупности проверок).

Выявление уязвимостей компонентов объекта обследования включает в себя формирование плана проверок, поиск уязвимостей, анализ обнаруженных уязвимостей и степени их влияния на защищенность объекта обследования.

Формирование плана проверок осуществляется средствами сканера безопасности.

В план включаются следующие проверки:

- определение известных уязвимостей операционных систем семейства Windows;
- проверка наличия удаленного доступа к приложениям;
- проверка наличия паролей по умолчанию;
- проверка известных уязвимостей NetBIOS и Registry;
- проверка наличия обновлений.

При наличии на узлах объекта обследования обнаруженных в ходе проверок сетевых сервисов дополнительно включается:

- проверка известных уязвимостей сервиса FTP;
- проверка известных уязвимостей сервиса RPC;
- проверка известных уязвимостей сервиса электронной почты;

- детальный анализ структуры и содержания веб-сайта, поддерживаемого http-сервером.

Результатом является сформированный средствами сканера безопасности детальный перечень проверок для каждого из обнаруженных узлов объекта обследования.

Поиск уязвимостей производится по окончании формирования плана проверок, путем запуска процесса сканирования и слежения за ходом его выполнения.

По результатам выполнения заданных проверок средствами сканера безопасности формируется сводный отчет в форме pdf.

Анализ обнаруженных уязвимостей и степени их влияния на защищенность объекта обследования осуществляется экспертным методом. При классификации и оценке степени опасности уязвимости разделяются на два класса:

- уязвимости реализации (Vulnerability);
- уязвимости конфигурации (Exposure).

Для эксплуатации уязвимостей конфигурации не всегда требуются специальные программные средства. Нарушитель может воспользоваться штатными средствами системы.

Производится анализ влияния каждой из обнаруженных уязвимостей на состояние безопасности объекта обследования в целом. Степень влияния оценивается по трехбалльной системе:

- низкая;
- средняя;
- высокая.

Результаты анализа уязвимостей приводятся в отчете об обследовании:

- класс уязвимости;
- перечень устройств, на которых обнаружена данная уязвимость;
- степень влияния на безопасность объекта обследования.

Результаты исследования безопасности корпоративной сети учреждения

Схема корпоративной сети государственного учреждения приведена на рис. 2.4.

Описание сети.

Корпоративная локальная сеть топологии типа «звезда». Сервер используется для обработки и хранения данных, поступающих с автоматизированных рабочих мест. Автоматизированные рабочие места объединены подключениями к маршрутизатору Cisco. Выход в закрытый сегмент сети ЕМТС происходит через криптошлюз «застава». Также в сети присутствует система обнаружения вторжений.

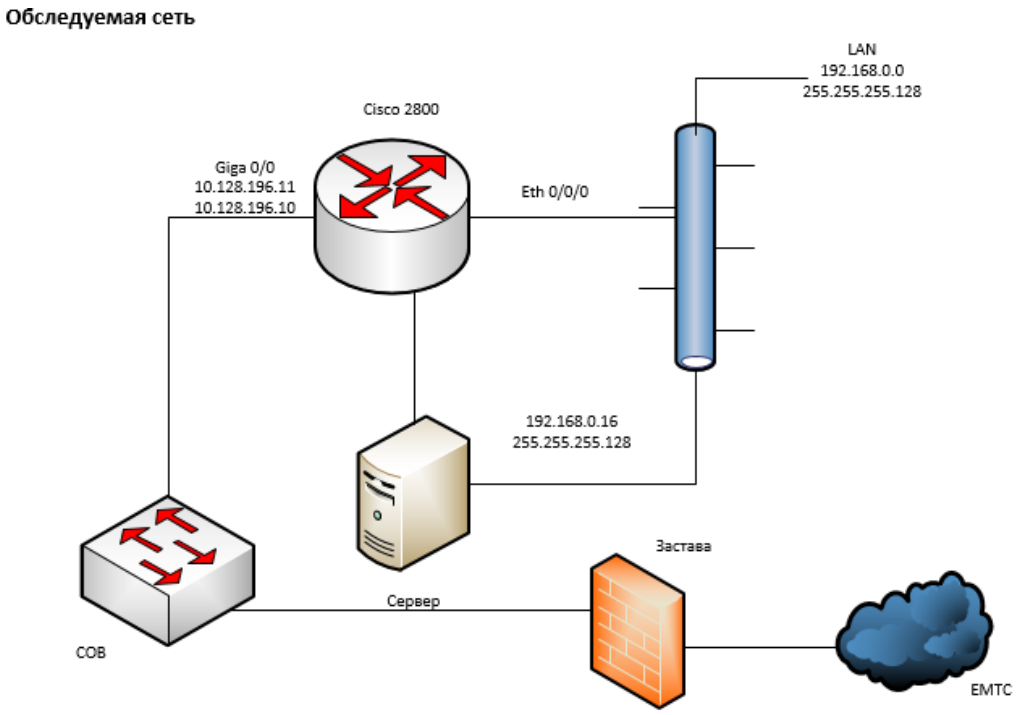


Рис. 2.4. Схема корпоративной сети государственного учреждения

При проведении инструментального анализа защищенности сети было проанализировано 36 узлов разной степени уязвимости (рис. 2.5).

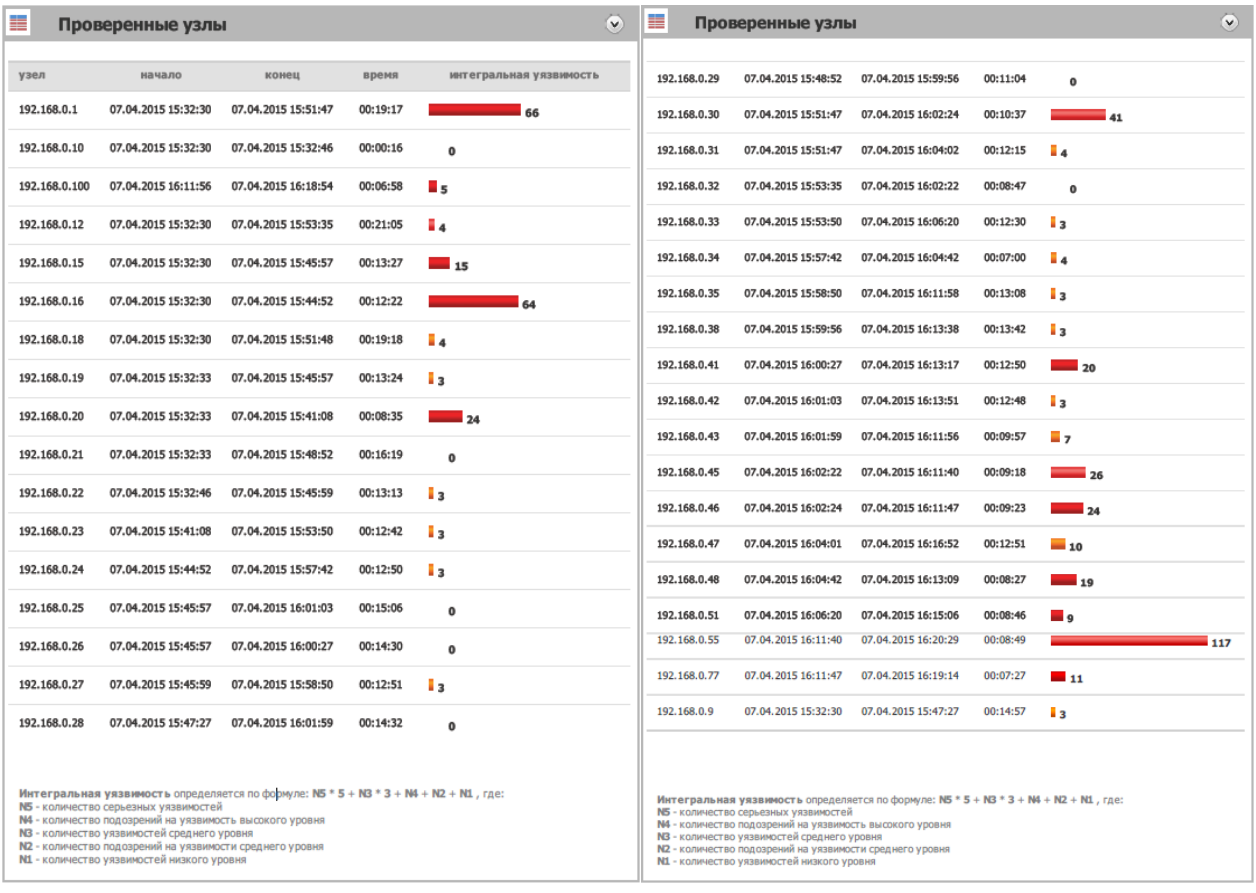
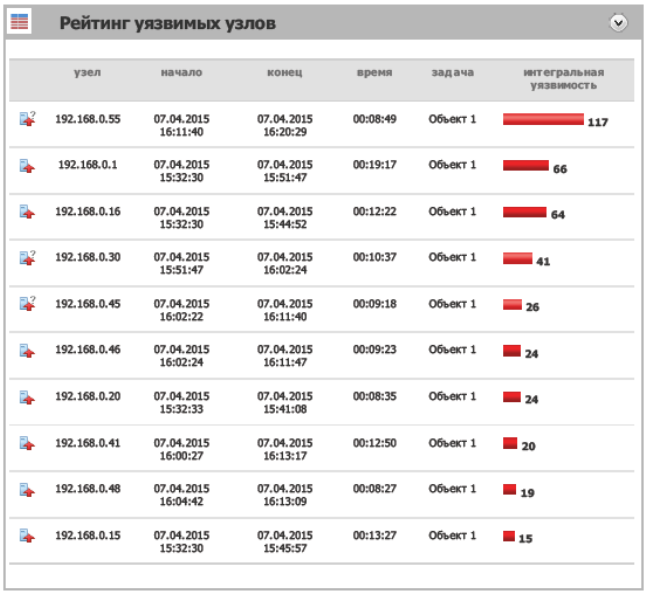


Рис. 2.5. Проверенные узлы

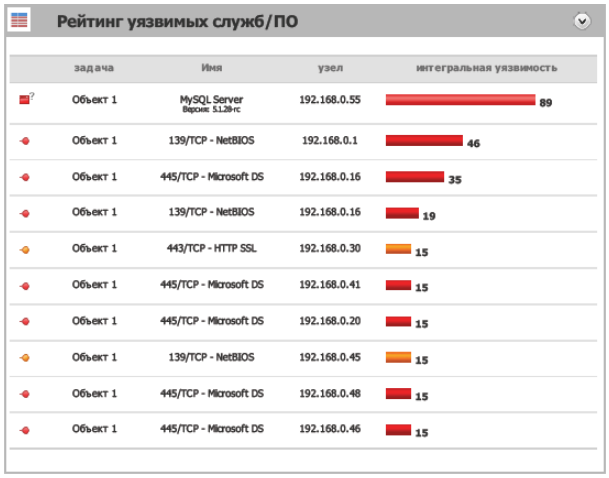
Наиболее уязвимые узлы приведены на рис. 2.6.
Наиболее уязвимые службы приведены на рис. 2.7.
Наиболее опасные уязвимости приведены на рис. 2.8.



Рейтинг уязвимых узлов

узел	начало	конец	время	задача	интегральная уязвимость
192.168.0.55	07.04.2015 16:11:40	07.04.2015 16:20:29	00:08:49	Объект 1	117
192.168.0.1	07.04.2015 15:32:30	07.04.2015 15:51:47	00:19:17	Объект 1	66
192.168.0.16	07.04.2015 15:32:30	07.04.2015 15:44:52	00:12:22	Объект 1	64
192.168.0.30	07.04.2015 15:51:47	07.04.2015 16:02:24	00:10:37	Объект 1	41
192.168.0.45	07.04.2015 16:02:22	07.04.2015 16:11:40	00:09:18	Объект 1	26
192.168.0.46	07.04.2015 16:02:24	07.04.2015 16:11:47	00:09:23	Объект 1	24
192.168.0.20	07.04.2015 15:32:33	07.04.2015 15:41:08	00:08:35	Объект 1	24
192.168.0.41	07.04.2015 16:00:27	07.04.2015 16:13:17	00:12:50	Объект 1	20
192.168.0.48	07.04.2015 16:04:42	07.04.2015 16:13:09	00:08:27	Объект 1	19
192.168.0.15	07.04.2015 15:32:30	07.04.2015 15:45:57	00:13:27	Объект 1	15

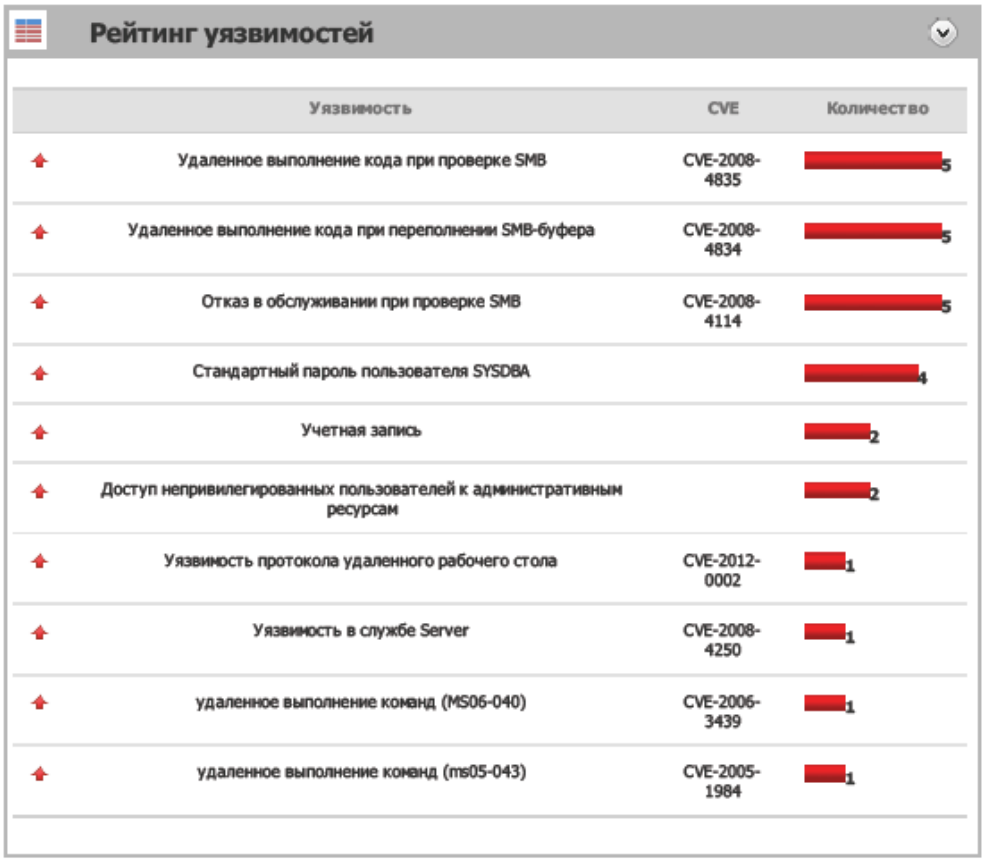
Рис. 2.6. Наиболее уязвимые узлы



Рейтинг уязвимых служб/ПО

задача	Имя	узел	интегральная уязвимость
Объект 1	MySQL Server Версия: 5.1.28-rc	192.168.0.55	89
Объект 1	139/TCP - NetBIOS	192.168.0.1	46
Объект 1	445/TCP - Microsoft DS	192.168.0.16	35
Объект 1	139/TCP - NetBIOS	192.168.0.16	19
Объект 1	443/TCP - HTTP SSL	192.168.0.30	15
Объект 1	445/TCP - Microsoft DS	192.168.0.41	15
Объект 1	445/TCP - Microsoft DS	192.168.0.20	15
Объект 1	139/TCP - NetBIOS	192.168.0.45	15
Объект 1	445/TCP - Microsoft DS	192.168.0.48	15
Объект 1	445/TCP - Microsoft DS	192.168.0.46	15

Рис. 2.7. Наиболее уязвимые службы



Рейтинг уязвимостей

Уязвимость	CVE	Количество
Удаленное выполнение кода при проверке SMB	CVE-2008-4835	5
Удаленное выполнение кода при переполнении SMB-буфера	CVE-2008-4834	5
Отказ в обслуживании при проверке SMB	CVE-2008-4114	5
Стандартный пароль пользователя SYSDBA		4
Учетная запись		2
Доступ непривилегированных пользователей к административным ресурсам		2
Уязвимость протокола удаленного рабочего стола	CVE-2012-0002	1
Уязвимость в службе Server	CVE-2008-4250	1
удаленное выполнение команд (MS06-040)	CVE-2006-3439	1
удаленное выполнение команд (ms05-043)	CVE-2005-1984	1

Рис. 2.8. Наиболее опасные уязвимости

Разработка рекомендаций по устранению обнаруженных уязвимостей

Рассмотрим наиболее опасные уязвимости, обнаруженные в ходе сканирования, и приведем рекомендации по их устранению.

1) «Удаленное выполнение кода при проверке SMB», «удаленное выполнение кода при переполнении SMB-буфера».

Описание. Уязвимость, связанная с удаленным выполнением кода, возникает при обработке специально сформированных SMB-пакетов в программе обработки Microsoft Server Message Block (SMB) Protocol. Для эксплуатации данной уязвимости не требуется аутентификация, что позволяет злоумышленнику эксплуатировать данную уязвимость, если он отправит специально сформированное сетевое сообщение компьютеру, на котором запущена служба Server. В случае успешной эксплуатации данной уязвимости злоумышленник получает полный контроль над системой. Большая часть попыток эксплуатации данной уязвимости приводит к отказу в обслуживании, но теоретически возможно удаленное выполнение кода.

2) «Отказ в обслуживании при проверке SMB».

Описание. Уязвимость, связанная с отказом в обслуживании, возникает при обработке специально сформированных SMB-пакетов в программе обработки Microsoft Server Message Block (SMB) Protocol. Для эксплуатации данной уязвимости не требуется аутентификация, что позволяет злоумышленнику эксплуатировать данную уязвимость, если он отправит специально сформированное сетевое сообщение компьютеру, на котором запущена служба Server. В случае успешной эксплуатации данной уязвимости злоумышленник может аварийно завершить работу системы и перезагрузить ее.

Рекомендации по устранению:

Требуется следовать рекомендациям по обновлению от производителя Microsoft:

- Обновление ms09-001 устраняет уязвимости путем проверки полей в SMB-пакетах.
- Обновление ms10-012 устраняет данные уязвимости, изменяя способ проверки SMB-запросов в SMB.

3) Стандартный пароль пользователя SYSDBA.

Описание. Пользователь 'SYSDBA' имеет стандартный пароль 'masterkey'.

Рекомендации по устранению**:**

Требуется изменить стандартный пароль на надежный.

4) «Учетная запись».

Описание. Найдена открытая учетная запись «public».

Рекомендации по устранению:

Закрыть доступ к учетной записи.

5) Доступ непривилегированных пользователей к административным ресурсам.

Описание. Пользователи, не являющиеся администраторами на машине, имеют доступ на запись в административный общий каталог.

Рекомендации по устранению:

Запретить доступ к административным ресурсам для непривилегированных пользователей или отключите административные ресурсы.

6) Уязвимость протокола удаленного рабочего стола.

Описание. Уязвимость, позволяющая удаленно выполнить код, существует в протоколе удаленного стола и связана с обращением к объектам памяти, которые были удалены или некорректно инициализированы. Используя данную уязвимость, злоумышленник может запустить произвольный код в целевой системе, вследствие чего он сможет установить программы; просмотреть, изменить или удалить данные; создать новые учетные записи с полными правами пользователя.

Рекомендации по устранению:

Требуется следовать рекомендациям по обновлению от производителя Microsoft.

Обновление ms12-020 устраняет уязвимости, изменяя способ обработки пакетов в памяти протоколом RDP и способ обработки пакетов службой RDP.

7) Уязвимость в службе Server.

Описание. Удаленное выполнение кода возможно в службе Server в системах Windows и возникает из-за некорректной обработки специально сформированных RPC-запросов. В случае успешной эксплуатации данной уязвимости злоумышленник может получить полный контроль над системой.

Рекомендации по устранению:

Требуется следовать рекомендациям по обновлению от производителя Microsoft.

Обновление MS08-067 для системы безопасности устраняет уязвимость, изменяя способ обработки RPC-запросов службой сервера.

8) Удаленное выполнение команд ms06-040.

Описание. В службе Server присутствует уязвимость переполнения буфера. Удаленный атакующий с помощью специальным образом сформированного запроса может вызвать отказ в обслуживании или выполнить произвольный код с системными привилегиями и получить полный контроль над системой.

Рекомендации по устранению:

Требуется следовать рекомендациям по обновлению от производителя Microsoft.

Обновление ms06-040 устраняет недавно обнаруженную уязвимость, о которой сообщалось в частном порядке, а также дополнительные проблемы, обнаруженные в результате внутреннего исследования.

9) Удаленное выполнение команд ms05-043.

Описание. Служба Spooler предназначена для управления принтерами и заданиями печати и экспортирует интерфейс на базе RPC (Remote Procedure Call). В данной службе присутствует уязвимость переполнения буфера. Удаленный или локальный пользователь может подключиться к системе через NULL-сессию и с помощью специального запроса выполнить произвольный код с привилегиями Local System или вызвать отказ в обслуживании. В системах Windows XP SP2 и Windows Server 2003 данная уязвимость не позволяет атакующему выполнить произвольный код – только отказ в обслуживании.

Рекомендации по устранению:

Требуется следовать рекомендациям по обновлению от производителя Microsoft.

Обновление ms05-043 устраняет недавно обнаруженную уязвимость, сообщение о которой было получено в частном порядке. В службе диспетчера очереди печати существует уязвимость, делающая возможным удаленное выполнение кода.

10) Доступ к ресурсам.

Описание. Непривилегированным пользователям доступна запись в общий ресурс. Возможно распространение сетевых вирусов.

Рекомендации по устранению:

Запретить доступ непривилегированным пользователям к общим ресурсам.

11) Не требуется подписывание SMB.

Описание. Узел не требует подписывания SMB. Возможно проведение атаки «человек посередине» на SMB-сервер.

В настройках SMB-сервера доступны три опции, касающиеся подписывания SMB:

a) подписывание SMB включено и обязательно для всех клиентов;
b) подписывание SMB включено, но не обязательно для всех клиентов;
c) подписывание SMB отключено.

Безопасность данных обеспечивает только первый вариант с включенным и обязательным для всех клиентов подписыванием SMB. На данном узле выбран небезопасный вариант настроек.

Рекомендации по устранению:

Включить подписывание SMB в настройках сервера.

12) Доступ по нулевой сессии.

Описание. Доступ по нулевой сессии позволяет злоумышленникам получить несанкционированный доступ к узлу с операционной системой, основанной на Windows NT (или ОС семейства UNIX с установленным пакетом Samba), введя пустое имя пользователя и пустой пароль. Если доступ по нулевой сессии разрешен, анонимный пользователь может получить большой объем информации о конфигурации системы (список общих

ресурсов, список пользователей, список рабочих групп и т. д.). Полученные данные в дальнейшем могут быть использованы для осуществления несанкционированного доступа.

Рекомендации по устранению:

Windows:

1. В разделе реестра HKEY_LOCAL_MACHINE\System\ CurrentControlSet\Control\LSA установите значение параметра RestrictAnonymous = 2 для Windows 2000/XP/2003 (1 для Windows NT3.5/NT4.0) (тип параметра – REG_DWORD).

2. Для Windows 2000/XP/2003:

В разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\lanmanserver установите значение параметра RestrictNullSessionAccess = 1 (тип параметра – REG_DWORD).

Для Windows NT3.5/NT4.0:

В разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\LanManServer\Parameters установите значение параметра RestrictNullSessAccess = 1 (тип параметра – REG_DWORD).

3. Перезагрузите систему для вступления изменений в силу.

Samba:

Разрешить доступ к серверу только зарегестрированным пользователям: в файле smb.conf изменить ключ security = share на security = user (или security = server или security = domain).

13) Разглашение информации.

Описание. Злоумышленники могут получить конфиденциальную информацию, не проходя авторизацию, с помощью запроса

NULL BASE.

Обратите внимание, что NULL BASE запрос необходим для корректной работы некоторых приложений. Например, в 3 версии протокола LDAP запрос используется для получения поддерживаемых сервером типов аутентификции и другой служебной информации.

Рекомендации по устранению:

Оцените степень критичности предоставляемой информации. При необходимости запретите использование запросов NULL BASE.

14) Подмена данных.

Описание. При использовании протокола Remote Desktop Protocol (RDP) в Microsoft Terminal Server закрытые ключи RSA хранятся в mstlsapi.dll и используются для подписывания сертификатов, что позволяет злоумышленникам, действующим удаленно, подменять открытые ключи доверенных серверов и проводить атаки типа «человек-посередине».

Для успешной эксплуатации злоумышленнику необходима возможность перехватывать трафик между терминальным сервером и терминальным клиентом.

Рекомендации по устранению:

Необходимо подключаться к терминальным серверам только через доверенные сети или использовать протокол TLS.

15) Рекурсия.

Описание. DNS-сервер поддерживает рекурсию запросов. При определенных обстоятельствах злоумышленник может вызвать на сервере отказ в обслуживании.

Рекомендации по устранению:

Разрешить рекурсию только для доверенных адресов.

16) Обход функций безопасности NLA.

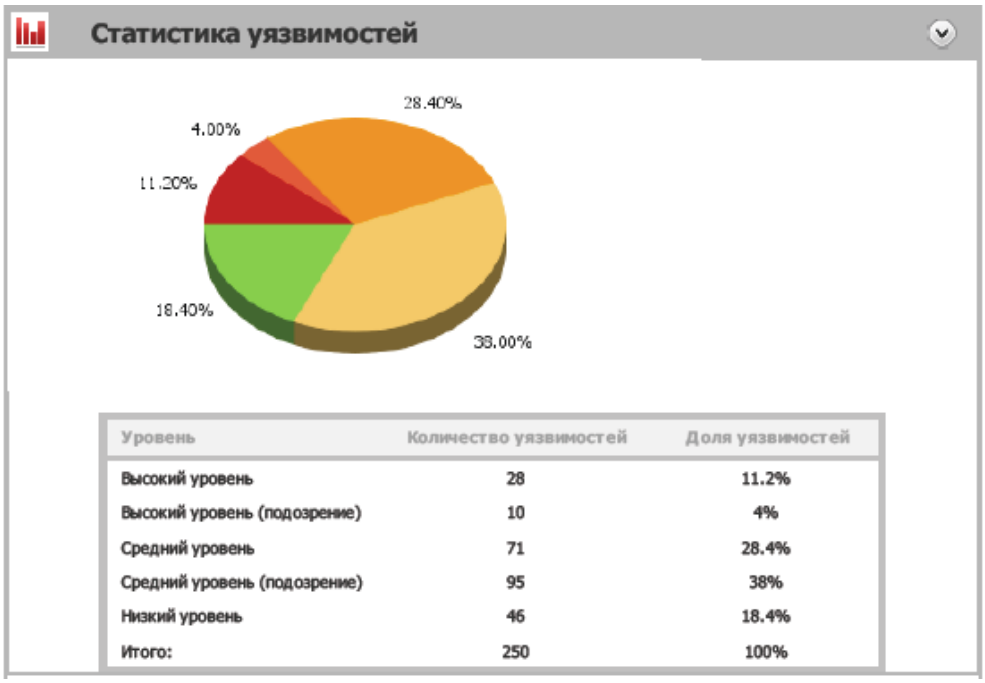
Описание. Уязвимость, позволяющая обойти механизм защиты, существует в службе сведений о подключенных сетях (NLA) и связана со смягчением политики межсетевого экрана и/или настроек некоторых служб, что расширяет область, доступную для атак. Уязвимость вызвана некорректной проверкой службой NLA компьютеров, подключенных к домену, на предмет их подключения к ненадежной сети.

Рекомендации по устранению:

Требуется использовать рекомендации производителя:

http://technet.microsoft.com/security/bulletin/ms15-005.

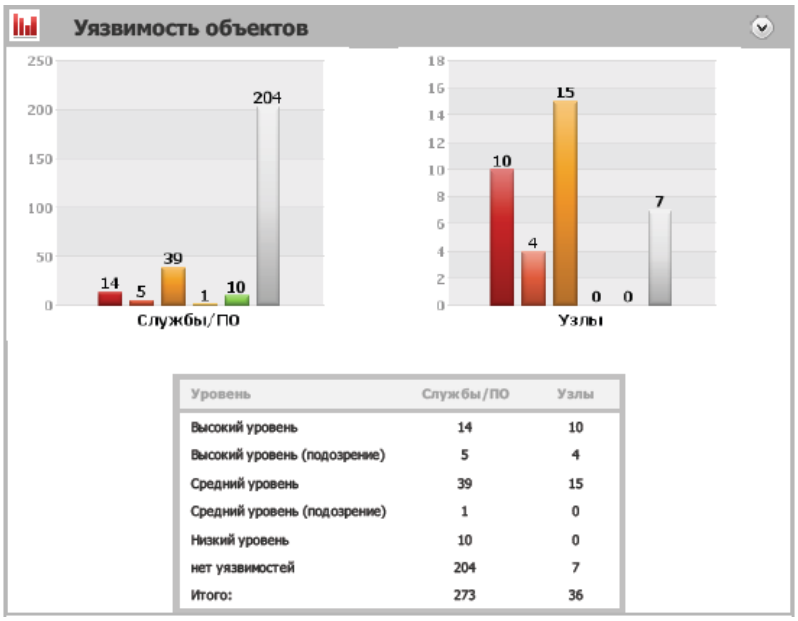
Перечень остальных обнаруженных уязвимостей и рекомендации по их устранению описаны в [5]. Общая статистика уязвимостей в сети приведена на рис. 2.9.



Уровень	Количество уязвимостей	Доля уязвимостей
Высокий уровень	28	11.2%
Высокий уровень (подозрение)	10	4%
Средний уровень	71	28.4%
Средний уровень (подозрение)	95	38%
Низкий уровень	46	18.4%
Итого:	250	100%

Рис. 2.9. Общая статистика уязвимостей в сети

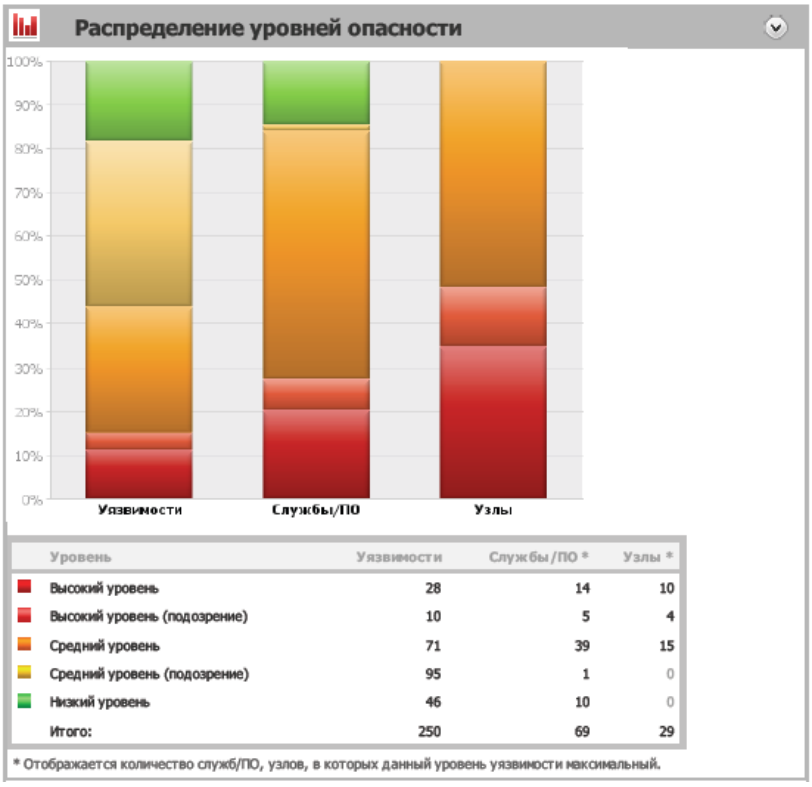
Общая статистика уязвимости объектов приведена на рис. 2.10.



Уровень	Службы/ПО	Узлы
Высокий уровень	14	10
Высокий уровень (подозрение)	5	4
Средний уровень	39	15
Средний уровень (подозрение)	1	0
Низкий уровень	10	0
нет уязвимостей	204	7
Итого:	273	36

Рис. 2.10. Общая статистика уязвимостей объектов

Распределение уровней опасности приведено на рис. 2.11.



Уровень	Уязвимости	Службы/ПО *	Узлы *
Высокий уровень	28	14	10
Высокий уровень (подозрение)	10	5	4
Средний уровень	71	39	15
Средний уровень (подозрение)	95	1	0
Низкий уровень	46	10	0
Итого:	250	69	29

* Отображается количество служб/ПО, узлов, в которых данный уровень уязвимости максимальный.

Рис. 2.11. Распределение уровней опасности

В результате проведения работ, согласно разработанным рекомендациям, была устранена основная часть обнаруженных уязвимостей, получены следующие результаты:

1. Оставшиеся после проведения работ уязвимости приведены на рис. 2.12.

2. Общая статистика уязвимостей в сети после проведения работ приведена на рис. 2.13.

Рис. 2.12. Оставшиеся после проведения работ уязвимости

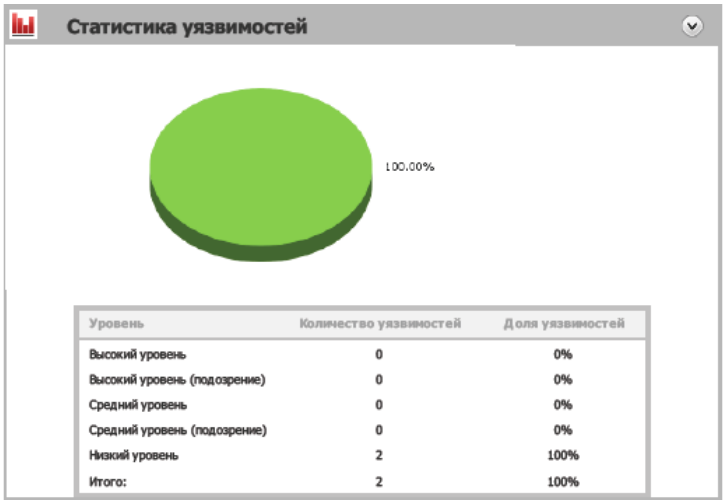


Рис. 2.13. Общая статистика уязвимостей в сети после проведения работ

3. Общая статистика уязвимости объектов после проведения работ приведена на рис. 2.14.

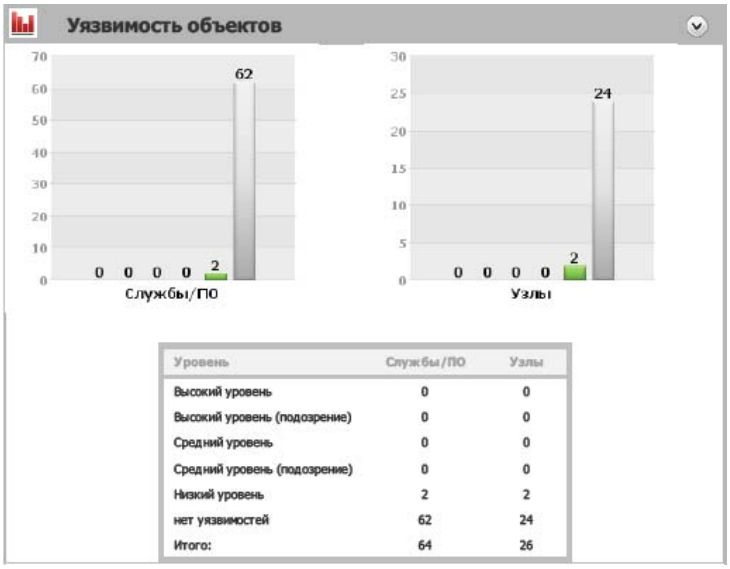


Рис. 2.14. Общая статистика уязвимости объектов после проведения работ

4. Распределение уровней опасности в сети после проведения работ приведена на рис. 2.15.

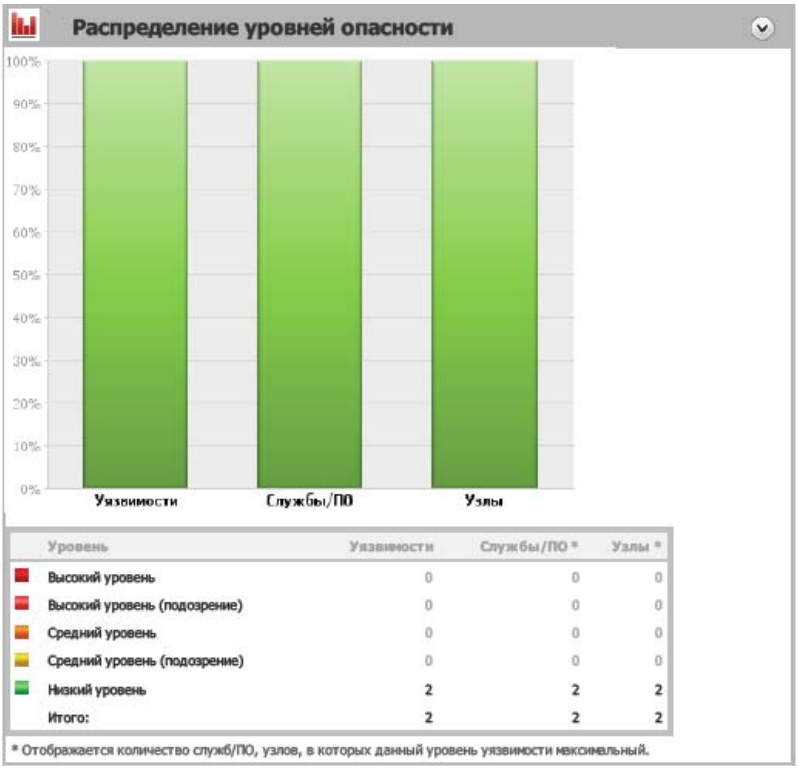


Рис. 2.15. Распределение уровней опасности в сети после проведения работ

Таким образом, работа по устранению уязвимостей привела к повышению уровня защищенности корпоративной сети учреждения.

Были устранены практически все обнаруженные уязвимости за исключением запущеного планировщика заданий и включенной маршрутизаци, требуемых для удобства работы с сетью, так как данные уязвимости не были оценены как критичные.

Исследование защищенности корпоративной сети учреждения показало, что инструментальные проверки являются высокоэффективными, при этом требуется производить постоянный мониторинг безопасности таких сетей, так как найденные на объекте уязвимости приводят к резкому снижению уровня защищенности.

В процессе исследования были разработаны рекомендации по устранению всех найденных уязвимостей, благодаря чему был значительно повышен уровень защищенности корпоративной сети государственного социально-ориентированного учреждения. При этом внедрения дополнительных средств защиты не требуется, так как найденные уязвимости устраняются с помощью настройки и обновления операционной системы и программного обеспечения.

Библиографический список

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения.
2. *Лепихин В.Б.* Сравнительный анализ безопасности. – URL: http://www.securitylab.ru/analytics/365241.php (дата обращения: 10.11.2015 г.).
3. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К): Утв. приказом Гостехкомиссии России от 30.08.02 № 282. – М., 2001.
4. Программа и методика проведения контроля за уровнем защищенности. – СПб.: СПбГУП: СПбИАЦ, 2014.
5. *Черток А.В.*, *Черток Е.В*. Анализ уязвимостей локальной сети и разработка рекомендаций по их устранению // Вопросы защиты информации. – 2015. – № 3. – С. 55-61.

2.2. Исследование уязвимостей Framework UI5 для SAP

В современном мире невозможно представить какой-либо бизнес-процесс или производство без использования информационных технологий. Информационные технологии все глубже проникают во все отрасли хозяйства, а также в повседневную жизнь человека. Эта интеграция с каждым годом происходит все быстрее, легче и масштабней, предоставляя людям уникальные технологии по ведению собственного бизнеса, такие как доступ с любой точки земли к необходимым ресурсам, бизнес-приложения, независимые от аппаратной платформы, большая скорость обмена информацией, дружественный интерфейс и т. д. Но с новыми технологиями появляются и риски использования этих технологий злоумышленниками в своих целях. Это возможно из-за содержания в новых технологиях новых (а порой, и старых) уязвимостей. Благодаря уязвимостям злоумышленники могут подорвать всю инфраструктуру подразделений, использующих актуальные методы информационных систем, и нанести непоправимый ущерб данным организациям или частным лицам. В связи с этим все чаще встает вопрос защиты информационных систем для ликвидации возможного риска и минимизации предполагаемого ущерба, что сэкономит как время, так и затраченные ресурсы.

В данном параграфе исследуются возможные виды атак на framework UI5 компании SAP, использующимся в большинстве ERP-систем данной компании, а также существующие методы противодействия этим атакам. Исследование проведено как с помощью автоматизированных средств, так и ручным способом. Предложены рекомендации

для создания и использования безопасных программ на основе фреймворка UI5. В качестве исследуемой ERP-системы с предустановленным фреймворком использовалась SAP HANA, наиболее распространенная высокопроизводительная платформа для работы аналитических и транзакционных приложений в режиме реального времени [1].

Актуальность данной работы состоит в том, что исследуемый фреймворк UI5 может иметь уязвимости, а вследствии этого большому количеству его пользователей может быть нанесен ущерб злоумышленниками. Если уязвимости будут найдены, то они составят автоматически брешь в защите топовых продуктов компании. SAP известна своей пользовательской аудиторией, по скромным подсчетам превышающей 12 миллионов человек [2] и имеющей представительство в более чем 130 странах мира. Автоматизированные системы компании используются в сфере финансов, торговли, бухгалтерском учете, логистике, в сфере управления персоналом и даже в медицине. Уязвимости в предлагаемом программном обеспечении поставят под угрозу инфраструктуру многих крупных компаний и корпораций, а также государственных служб.

Место framework SAP UI5 в инфраструктуре SAP HANA

SAP SE является мировым лидером по производству программного обеспечения. Компания занимается разработкой автоматизированных систем управления такими внутренними процессами предприятия, как бухгалтерский учет, торговля, производство, финансы, управление персоналом, управление складами и т. д. Приложения обычно можно адаптировать под правовой контекст определенной страны.

ERP-системы компании SAP представляют собой многопользовательские модульные системы, обеспечивающие сбалансированное управление ресурсами организации, не только относящиеся к основной деятельности производственного предприятия, но и объединяющие посредством общей модели данных данные о производстве, закупках, сбыте, финансах, кадрах [3].

Для исследования возможностей фреймворка SAP UI5 требовалась любая современная ERP-система со встроенным данным компонентом в ней. Для этого отлично подходила и была выбрана система SAP HANA.

SAP HANA – это современная платформа SAP, использующая для вычислений оперативную память и предназначенная для выполнения аналитики в режиме реального времени (технология «In Memory») [4] и разработки и развертывания приложений реального времени. Она позволяет организациям анализировать бизнес-операции, использующие большой объем разнообразных подробных данных, буквально «со скоростью мысли», что открывает новые возможности для ведения бизнеса.

В 2010 г. SAP начала подготовку к переходу на новый пользовательский интерфейс. В качестве технологии была выбрана связка HTML5 и Javascript. Таким образом, родился продукт SAP UI5.

SAP User Inteface HTML5 (SAP UI5) – это JavaScript-фреймворк для:

- построения пользовательских интерфейсов,
- обмена данными с SAP по протоколу OData,
- быстрого создания внутрикорпоративных порталов.

Ключевыми особенностями данного фреймворка являются [5]:

- высокая производительность,
- полностью документированный API на английском языке,
- гибкие возможности по оформлению,
- использование JavaScript библиотеки jQuery.

SAP UI5 включает в себя специальную библиотеку для мобильных устройств – sap.m, которая поддерживает такие мобильные операционные системы, как iOS, BlackBerry и Android. Поддержка, естественно, подразумевается именно в браузере.

Исследование источников угроз

Для того чтобы выявить возможные источники угроз фреймворка SAP UI5 использовался список наиболее часто встречающихся угроз в приложениях – OWASP TOP 10.

Open Web Application Security Project (OWASP) – это открытый проект обеспечения безопасности веб-приложений. Сообщество OWASP включает в себя корпорации, образовательные организации и частных лиц со всего мира. Сообщество работает над созданием статей, учебных пособий, документации, инструментов и технологий, находящихся в свободном доступе. Участники проекта уже десять лет составляют список Топ-10 самых опасных уязвимостей в веб-приложениях, стараясь привлечь внимание всех веб-разработчиков [6].

Список угроз OWASP TOP 10:

- Уязвимость внедрения кода.
- Некорректная аутентификация и управление сессией.
- Межсайтовый скриптинг.
- Небезопасные прямые ссылки на объекты.
- Небезопасная конфигурация.
- Утечка чувствительных данных.
- Отсутствие контроля доступа к функциональному уровню.
- Подделка межсайтовых запросов.
- Использование компонентов с известными уязвимостями.
- Неваледированные перенаправления.

Детальное рассмотрение этих уязвимостей показало их уникальность как в возможном случае использования атакующими, так и в случае при-

менения защиты. Многие уязвимости, учитывая свою специфичность и величину программного продукта SAP UI5, продуктивней будет искать автоматизированными средствами. Оставшуюся часть легче будет найти ручным способом. Важно при поиске векторов атак сконцентрироваться на возможных критичных сервисах, так как они являются первоочередными целями злоумышленников.

Используемый инструментарий

В итоге процесс поиска возможных векторов атак разбился на следующие подцели:

- Установка необходимой программной среды для работы с SAP UI5.
- Изучение возможности создания программ на основе SAP UI5.
- Поиск уязвимостей в созданных программах.
- Ручной поиск уязвимостей в самом фреймворке.
- Автоматизированный поиск уязвимостей в самом фреймворке.

Решено было исследовать фреймворк на примере написания собственных приложений на языке XSJS.

XSJS – язык программирования от компании SAP, разработанный для создания проектов на основе SAP UI5. Этот язык является немного модифицированной версией языка JavaScript, с добавлением специальных возможностей конфигурации проектов. Программы, написанные на данном языке, имеют расширение «.xsjs».

Для создания приложений для SAP HANA используются готовые решения от компании Eclipse. Из готовых решений можно выбрать Eclipse Luna или Eclipse Kepler, которые подходят для создания проектов на основе SAP UI5. Выбор пал на решение Eclipse Luna.

Для исследования UI5 на возможные уязвимости из OWASP TOP 10 были написаны программные приложения для:

- отправки HTTP запроса (рис. 2.16);
- просмотра базы данных SAP HANA Studio (рис. 2.17).

В ходе проверки данных приложений было выяснено, что если приложение написано без специализированной защиты с использованием безопасных библиотек, в случае когда разработчик не в курсе о существующих опасностях, то они подвержены уязвимостям: внедрения кода, некорректной аутентификации и управления сессией, межсайтовому скриптингу, подделке межсайтовых запросов. Рекомендации использования безопасных библиотек приведены только в специализированных руководствах безопасности от компании SAP и не доступны без корпоративной учетной записи.

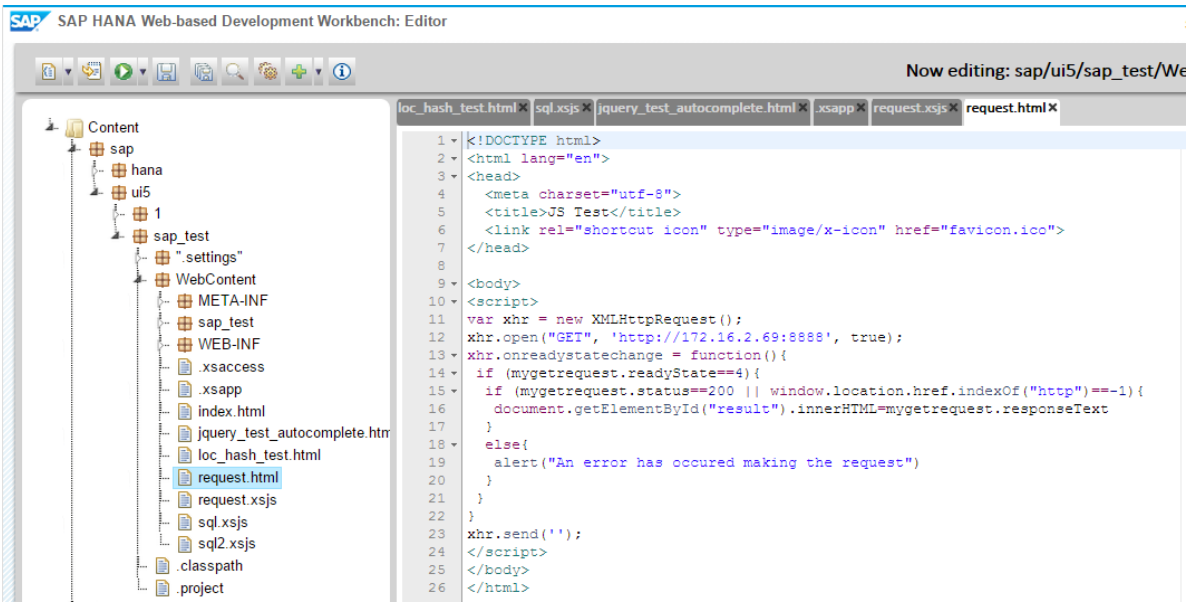


Рис. 2.16. Приложение для отправки HTTP запроса

В ходе ручного поиска уязвимостей в самом фреймворке SAP UI5 было обнаружено, что используемая встроенная библиотека jQuery не обновлена до актуальной версии (в фреймворке используется версия jQuery 1.7.1, а актуальная версия 1.11.3). В частности, версия 1.7.1 подвержена атаке DOM Cross Site Scripting в селекторе с атрибутом класса ('. XSS_VECTOR') [7]. Она выполнима, когда пользователь контролирует значение, которое передается как выбранный класс в селекторе. Также в версии 1.7.1 существует похожая уязвимость, когда селектор интерпретируется как HTML [8]. Это может являться вектором для осуществления атак на компоненты с известными уязвимостями.

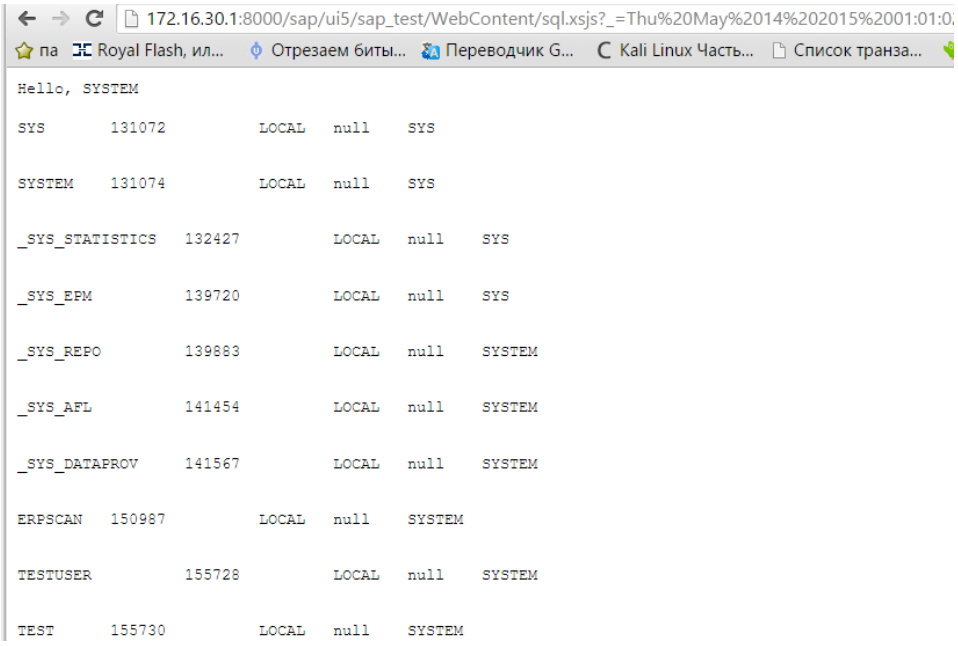


Рис. 2.17. Приложение для просмотра базы данных

Для автоматизированного поиска уязвимостей в фреймворке было использовано готовое решение – анализатор исходного кода CheckMarx CxSAST.

CheckMarx CxSAST является мощным анализатором исходного кода и решением, предназначенным для выявления отслеживания и фиксации технических и логических брешей безопасности в исходном коде.

В ходе сканирования фреймворка SAP UI5 были выявлены мелкие недочеты, но не было найдено ни одной серьезной уязвимости. Как и в случае с ручным сканированием, CheckMarx указал на устаревшую версию библиотеки jQuery, но данный недочет уже был рассмотрен выше.

Возможные методы защиты

В ходе исследования были найдены возможные реализации уязвимостей программ, написанных на языке XSJS. Для предотвращения возможных векторов атак рассмотрим предлагаемые встраиваемые методы защиты.

Система SAP HANA позволяет определить доступ к каждому отдельному пакету приложений, который необходим для разработки и развертывания собственного приложения. Для недопущения реализации уязвимости некорректной аутентификации и управления сессией, а также уязвимости внедрения кода следует сконфигурировать специальный файл «доступ к приложению», с расширением «.xsaccess».

Для недопущения возникновения уязвимости межсайтового скриптинга компания SAP предлагает встроенные библиотеки защиты UI5 XSSEncoder. Используя данную библиотеку, необходимо заэкранировать небезопасные параметры. Экранирование различных параметров зависит от типа представления этого параметра.

Для защиты от уязвимости подделки межсайтовых запросов необходимо использовать параметр prevent_xsrf в файле «доступ к приложению».

Для закрытия уязвимости DOM Cross Site Scripting необходимо будет использовать последнюю версию SAP HANA с предустановленным фреймворком UI5 (эта уязвимость была исправлена в новых версиях программы).

Для защиты самого фреймворка необходимо своевременно скачивать обновления безопасности и устанавливать их. Несоблюдение этого может привести к появлению возможной уязвимости и предоставлению злоумышленнику возможности для осуществления вектора нападения на системы.

Библиографический список

1. Блог компании SAP [Электронный ресурс]. – URL: http://habrahabr.ru/company/sap/blog/252539/ (дата обращения: 09.11.2015).

2. SAP [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/SAP (дата обращения: 09.11.2015).
3. Википедия, ERP [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/ERP (дата обращения: 09.11.2015).
4. SAP Hana: технический обзор [Электронный ресурс]. – URL: http://www.novardis.com/netcat_files/366/653/h_9a0f043ed9489f4e1cb7f7e82e638c98 (дата обращения: 09.11.2015).
5. Знакомство с SAPUI5 [Электронный ресурс]. – URL: http://sapland.ru/articles/stats/2013/1/otobrazhenie-tekuschego-vremeni-v-sap-hana-s-pomoschiyu-radarnoi-diagrammi-2.html (дата обращения: 09.11.2015).
6. Обзор площадки для тестирования веб-уязвимостей OWASP Top-10 [Электронный ресурс]. – URL: http://habrahabr.ru/post/250551/ (дата обращения: 09.11.2015).
7. jQuery Versions Vulnerable to Selector XSS with class Attribute [Электронный ресурс]. – URL: http://goo.gl/GPc4tt (дата обращения: 09.11.2015).
8. jQuery Bug Tracker Ticket #11290 [Электронный ресурс]. – URL: http://goo.gl/WAmzNj (дата обращения: 09.11.2015).

2.3. Исследование уязвимостей корпоративного решения SAP Afaria

Современные организации и предприятия для оптимизации работы, снабжают своих сотрудников многофункциональными мобильными устройствами, которые позволяют им быть неотрывными от процесса производства и оперативно принимать решения. Существует множество готовых решений для управления и защиты корпоративных носимых устройств, но лидером в данной области является Sap Afaria.

Afaria – это MDM решение, которое позволяет обеспечивать контроль и защиту мобильных устройств, используемых организацией и ее сотрудниками. Управление мобильными устройствами служит для того, чтобы обеспечивать безопасность корпоративных данных на устройствах, находящихся вне сетевой инфраструктуры, а также контролировать состояние самих устройств [1].

Gartner Magic Quadrant в 2014 г. назвала Afaria самым лучшим решением для управления мобильными устройствами.

Для исследования была подготовлена лабораторная среда, состоящая из сервера, эмулятора телефона и телефона (рис. 2.18).

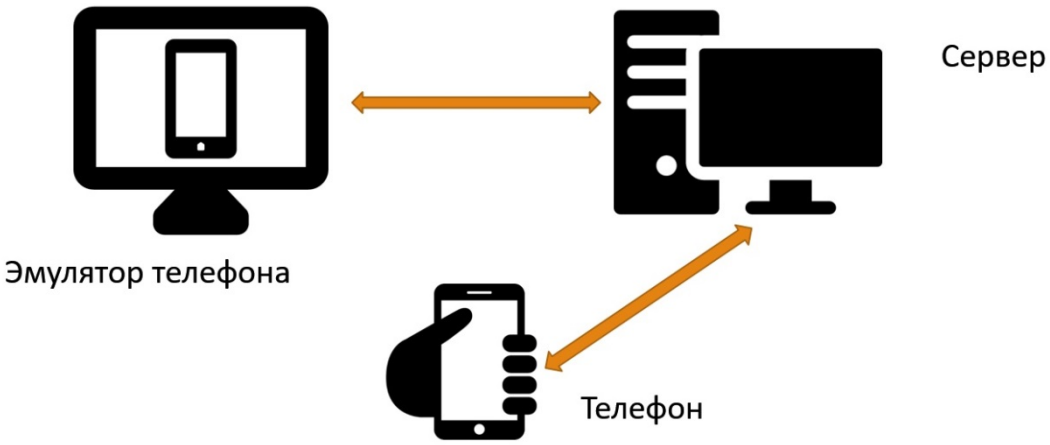


Рис. 2.18. Схема лабораторной среды

В качестве сервера, указанного на схеме, в виртуальной машине ОС Windows Server 2008 SP1, было установлено корпоративное приложение SAP Afaria версии 7.0 SP5, выпущенное в августе 2014. Для исследования на телефоне и в эмуляторе использовалось программное обеспечение платформы Android 5.0. Телефон и эмулятор были привязаны к серверу Afaria с помощью клиентской программы Afaria Client for Android, по средствам настройки через специальные коды, которые создаются администратором через политику Enrollment policy.

В ходе исследования интерес представляла прежде всего возможность скомпрометировать устройства клиентов, для этого была рассмотрена работа серверной части, изучены протоколы общения между мобильными устройствами и сервером, опробованы функциональные возможности Afaria.

Начальный этап исследования состоял из проверки веб-интерфейса портала Afaria. Были проведены проверки на защищенность от атак типа: XSS, CSRF, Clickjacking, SQL Injection.

В результате проверки было выявлено, что разработчик следует общепринятым рекомендациям написания безопасного кода. Таким образом, во всех полях, в которые у пользователей существует доступ на запись, имелись проверки на вредоносное внедрение кода [2], которые успешно прошли проверку на наличие ошибок разработчика. Защита разработчиком от CSRF реализовалась с помощью использования во всех пакетах так называемых CSRF токенов, что в полной мере защищает от подделки межсайтовых запросов [3]. В случае с защитой от атак вида SQL Injection, разработчиком было принято решение вынести сервис, отвечающий за запросы к базе данных, отдельно от системы, где располагался интерфейс управления сайтом, весь трафик, идущий между пользовательским интерфейсом и сервисом для запросов к базе данных, был преобразован несколькими способами и защищен от подделки запросов с помощью токе-

нов и постоянно изменяющихся идентификаторов, поэтому выполнение данной атаки практически невозможно.

В системе не были найдены файлы, которые бы хранили пароли в открытом виде. Однако были найдены файлы, которые хранят пароли в зашифрованном виде, используя для шифрования статичный ключ. Так, например, при установке серверной части, устанавливается также клиент Afaria для Windows, в конфигурационных файлах которого хранится в зашифрованном виде пароль от сервисной учетной записи рабочей станции. Для шифрования пароля используют алгоритм Blowfish с фиксированным ключом «g9rlp»

Таким образом, злоумышленник, способный читать файлы с сервера, может получить доступ к критичному аккаунту и использовать его для дальнейшей компрометации.

Также часть данных в зашифрованном виде может быть обнаружена в реестре. Так, например, пароль от БД расположен в ветке HKLM\SOFTWARE\Wow6432Node\Afaria\Afaria\Server\Logging\Database\assword

В мобильном устройстве, которое использовало приложение для подключения к серверу Sap Afaria, в открытом доступе был найден незашифрованный лог файл, хранящий конфиденциальную информацию: телефонные номера, смс сообщения, данные о перемещениях и т. д.

В ходе исследования исходного кода системы (напомним, что серверная часть написана на C#, а в качестве клиента мы рассматриваем Android приложение Afaria) были найдены различные участки, которые так или иначе используют предопределенные значения для работы механизмов шифрования, что, конечно, не может положительно сказаться на их надежности.

Для примера будет рассмотрена уязвимость функционирования системы управления телефоном с помощью смс [4].

На сервере настраивается возможность отправки SMS либо через специальные SMPP (Short Message Peer-to-Peer) сервисы, либо через подключенный GSM модем.

Используя SMS команды, администратор может выполнить следующие действия:

- Заблокировать телефон.
- Стереть все данные с телефона (wipe).
- Разблокировать телефон.
- Запросить лог файл.
- Заблокировать пользователя.
- Послать сообщение.
- Сообщить о своем местоположении.

- Применить новую политику
- и т. д.

Критичность в том, что даже простое логирование данных в этом приложении не ограничено самим приложением, в журнал идут все данные с телефона, вплоть до SMS пользователей, телефонных звонков и состояния телефонного счета.

Конечно, разработчики Afaria предусмотрели аутентификацию в SMS сообщениях. Итак, например, SMS сообщение на блокировку пользователя выглядит примерно вот так:

@#!Afaria64aACAhntVzjTIjhHDMGql8ldvc/8U6IlIoPU7aAOT8=$\$CMD:USERLOCK

Давайте разберем данное сообщение:

@#!Afaria – сигнатура для мобильного приложения Afaria того, что это сообщение необходимо обработать.

64aACAhntVzjTIjhHDMGql8ldvc/8U6IlIoPU7aAOT8= – base64 строчка, по которой происходит аутентификация SMS.

$\$CMD – идентификатор, обозначающий, что SMS содержит команду.

USERLOCK – сама команда.

В результате изучения исходного кода была выявлена схема генерации данного сообщения.

SMS имеет следующий формат:

@#!Afaria+base64(sha256(<ClientID>+<ClientID>+<TransmitterID>+$\$CMD: +<CMD_NAME>))+$\$CMD:+ <CMD_NAME>

- <ClientID> – ID мобильного устройства.
- <TransmitterID> – Transmitter ID.

TransmitterID атакующий может получить анонимно, если отправит запрос на соединение с Afaria сервером.

ClientID, который представляет собой типичный GUID – строку вида {10F6592C-79E0-4E1D-868A-6921F27C7004}, создается на основе IMEI мобильного устройства.

Таким образом, все, что нужно знать атакующему для того, чтобы скомпрометировать телефон (заблокировать его) – IMEI жертвы.

Конечно, IMEI нельзя считать надежным и секретным, так как многие приложения, установленные на телефоне, могут получить эту информацию, более того, многие приложения пересылают IMEI в открытом виде на свой сервер с целью сбора статистики работы приложения. Скажем более, если компания закупила телефоны большой партией, то их IMEI будут различаться незначительно.

Результаты проведенного исследования уязвимостей корпоративного решения SAP Afaria приведены в табл. 2.4.

Таблица 2.4

Выявленные уязвимости SAP Afaria

Название уязвимостей	Количество
Небезопасное хранение критичных данных	4
Ошибки и закладки в исходном коде сервисов и приложения	3
Отказ в обслуживании и переполнение буфера	2
Отсутствие проверки авторизации	2
Небезопасная реализация соединения телефона и сервера	2

В ходе проведения исследования уязвимостей корпоративного решения были найдены уязвимости, позволяющие нанести огромный вред предприятию, использующему данную систему для управления мобильными устройствами. Найденные уязвимости были отправлены разработчику для исправления ошибок, влекущих за собой угрозы для организаций, использующих данное приложение.

Результат исследования служит для повышения уровня защищенности корпоративного решения Sap Afaria. Анализ безопасности корпоративного решения Sap Afaria показал, что защита информации должна происходить также и на уровне приложений, которые обрабатывают эти данные.

Библиографический список

1. Управление мобильными устройствами [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/Управление_мобильными_устройствами (дата обращения: 01.06.2015).
2. XSS глазами злоумышленника [Электронный ресурс]. – URL: http://habrahabr.ru/post/66057/ (дата обращения: 01.06.2015).
3. Типичные ошибки при защите сайтов от CSRF-атак [Электронный ресурс]. – URL: http://habrahabr.ru/post/235247/ (дата обращения: 01.06.2015).
4. SAP Afaria. Маленькая SMS для взлома большой компании [Электронный ресурс]. – URL: http://habrahabr.ru/company/dsec/blog/ 267907/ (дата обращения: 09.11.2015).

2.4. К вопросу решения задачи увеличения количества задействованных функций при тестировании программ в рамках контроля недекларированных возможностей

Одним из важнейших этапов процесса сертификации программных комплексов является тестирование. Тестирование программных продуктов представляет собой совокупность специфических мероприятий, таких как динамическое тестирование, статический анализ, тестирование надежности функционирования и др. Тестирование должно проводиться в соответствии с ГОСТ Р ИСО/МЭК 12119–2000 «Информационная технология. Пакеты программ. Требования к качеству и тестирование» и другими нормативными документами.

Для проведения качественной проверки работы и надежности продукта вышеперечисленные действия должны проводиться в полном объеме, с использованием вспомогательных сертифицированных программных инструментов.

Возникает серьезное препятствие на пути работы специалистов по сертификации, тестированию программных продуктов. Оно заключается в том, что любой программный комплекс состоит из значительного количества компонентов: тысяч файлов, десятка тысяч функций. Следовательно, проверка корректности работы всех функций, составляющих исходный код программы, физически невозможна в сжатые сроки, отведенные на сертификацию, по причине высокой трудоемкости выполняемой работы.

Исходя из данного факта, можно утверждать, что в процессе сертификации программного продукта проверяются только основные функции, от которых напрямую зависит корректная работа комплекса. Следовательно, остальные функции, тестирование которых не проводилось, потенциально могут являться причиной возникновения и, в последующем, реализации угроз информационной безопасности.

Для того чтобы выявлять недекларированные возможности программного продукта в процессе его тестирования, специалистам испытательной лаборатории стоит стремиться к анализу наибольшего количества функций. Для этого следует выстроить иерархию функций исходного кода программы – от высокоуровневых до низкоуровневых. Затем проверить корректность работы заявленных функций, результаты, к которым приводит их выполнение. Следующим этапом становится проверка работы тех функций, которые также прописаны в программе, но не были задействованы в процессе тестирования заявленных функций. Данные объекты могут не только отражать избыточность кода программы, но и являться причиной возникновения уязвимостей в тестируемом программном продукте.

Данный метод анализа исходных текстов программ крайне трудоемок, поэтому эксперты, занимающиеся сертификацией программных продуктов, прибегают к использованию автоматизированных систем анализа (анализаторов) для упрощения проводимых мероприятий. К сожалению, в существующих на данный момент анализаторах недостаточно эффективно реализованы методики поиска недекларированных возможностей. Отчасти данная проблема обусловлена тем, что при проведении сертификации заказчиком предоставляется недостаточно полный комплект документов, необходимых для проверки продукта на наличие программных закладок.

В связи с возникающими трудностями зачастую специалистам испытательных лабораторий приходится прибегать к ручному анализу исходных текстов программных продуктов. В процессе проведения данного типа анализа (как и при проведении прочих проверок) возникает потребность в использовании некого программного инструмента, который бы автоматизировал процесс документирования информации о проводимых мероприятиях, тем самым снижая затраты на проведение тестирования и облегчая работу экспертов. Подобный инструмент должен быть построен на основе использования специфической базы данных учета проделанных проверок и действий, которая, возможно, должна быть разработана на базе анализатора исходных текстов программ, или же как отдельный программный инструмент.

Специфика подобной базы данных состоит в том, что у эксперта по сертификации должна быть возможность не только последовательно вводить данные о проведенных проверках, но и добавлять новые проверки в уже заполненные разделы отчета.

Кроме того, информация, которая будет занесена в базу данных, должна сформировываться с помощью программных средств в отчет о проведенных проверках, оформленный в соответствии с ГОСТ 2.105–95 «Единая система конструкторской документации. Общие требования к текстовым документам». Это значительно облегчит работу специалистов по сертификации программных продуктов, снизив трудоемкость мероприятий по созданию отчетов о проведенных проверках в рамках тестирования программного продукта. Так как каждая проверка при использовании данного механизма оформления отчетов будет грамотно отображена в документе, любой независимый эксперт будет иметь возможность разобраться в результатах проделанной работы.

Подобный программный продукт разрабатывается специалистами испытательной лаборатории ОАО «Ассоциация специалистов информационных систем» и проходит стадию отладки.

2.5. Использование интерактивного дизассемблера IDA Pro для обнаружения модификации сегмента кода во время выполнения программы в операционной системе Windows

Модифицируемый код, с одной стороны, противоречит канонам программирования, по которым код – это код, и его следует исполнять, а данные – это данные, и их следует читать, а также при желании модифицировать. Но, с другой стороны, есть принцип фон Неймана, при грубой трактовке которого нет принципиальной разницы между данными и кодом – все это лишь последовательность байтов и битов.

Код, изменяющий свои собственные инструкции во время выполнения, будем называть самомодифицирующимся.

В операционной системе (ОС) MS-DOS модификация кода во время исполнения – совсем простое дело. Там можно менять содержимое ячейки вне зависимости от содержания в ней данных или кода. В ОС Windows код напрямую модифицировать запрещено и, вроде бы, все пути к модификации собственного кода закрыты. Однако выход есть, и не один.

Наиболее популярным (но не самым простым) методом модификации кода во время выполнения программы является изменение сегмента кода – это великолепный прием, позволяющий сокрыть истинные намерения программы. Подобный вид модификации встречается во многих вирусах, защитных механизмах, сетевых червях и прочих программах подобного типа.

В процессе исследования программы, производящей модификацию кода во время выполнения, дизассемблер отображает ее в том виде, в котором она была получена на момент снятия дампа или загрузки исходного файла, рассчитывая на то, что ни одна из машинных команд не изменится в ходе своего выполнения. Если модификацию вовремя не обнаружить, то реконструкция алгоритма будет выполнена неверно.

В связи с этим возникла задача: на базе интерактивного дизассемблера IDA Pro разработать плагин для поиска модификации сегмента кода во время выполнения программы в ОС Windows.

Проблемы модификации сегмента кода в ОС Windows

Для выполнения программы она должна быть помещена в память компьютера. В памяти компьютера содержатся и данные, которые могут использоваться исполняемой программой. Нет никакого различия между командами микропроцессора и данными. В определенных ситуациях команды программы могут рассматриваться как данные и, наоборот, данные становятся фрагментами программы. Таким образом, нет никакого препятствия к тому, чтобы программа в процессе выполнения изменяла саму себя [1].

Рассвет эпохи модификации кода во время выполнения программы пришелся на систему MS-DOS, программистами широко использовался подобный код, без которого не обходилась практически ни одна серьезная защита. Да и не только защита, он встречался в компиляторах, компилирующих код в память, распаковщиках исполняемых файлов, полиморфных генераторах и т. д. Во времена отладчиков типа debug.com модификация действительно серьезно затрудняла анализ, однако с появлением IDA Pro и Turbo-Debugger все изменилось.

Уже к середине девяностых годов начался массовый переход пользователей с MS-DOS на Windows 95/Windows NT, и разработчикам пришлось задуматься о переносе накопленного опыта и приемов программирования на новую платформу – от бесконтрольного доступа к памяти и компонентам операционной системы пришлось отвыкать [2].

Примеры модификации сегмента кода
во время выполнения программы в ОС MS Windows

Требование модификации атрибутов доступа к сегменту означает, что программа должна быть скомпилирована с указанием дополнительных атрибутов доступа к сегменту, непредусмотренных по умолчанию, либо в процессе выполнения программы должна быть вызвана функция Windows API VirtualProtect / VirtualProtectEx для добавления этих атрибутов. Выделение необходимого количества памяти для нового кода означает, что данный вид модификации позволяет выделить кусок адресного пространства произвольной длины (в рамках сегмента) под новый код. Иначе модификация производится в рамках статического буфера.

Ниже приведены различные варианты модификации кода во время выполнения [1].

Модификация сегмента кода с использованием функции WriteProcessMemory. Один из способов модификации кода во время исполнения – это использование API-функции WriteProcessMemory. С ее помощью можно писать данные в адресное пространство процесса. Область, куда предполагается писать, должна быть доступна для записи, в противном случае записи не произойдет. Прежде всего, с помощью данной функции вы исправляете код текущего процесса, но не можете увеличить объем памяти, чтобы добавить новый код.

```
.586P
.MODEL FLAT,STDCALL
PROCESS_VM_OPERATION  =    0008H
PROCESS_VM_WRITE      =    0020H
PROCESS_VM_OW     =    PROCESS_VM_OPERATION     OR
PROCESS_VM_WRITE
```

```
includelib E:\masm32\lib\user32.lib
includelib E:\masm32\lib\kernel32.lib
EXTERN OpenProcess@12:NEAR
EXTERN WriteProcessMemory@20:NEAR
EXTERN GetCurrentProcessId@0:NEAR
;-----------------------------------------------
_DATA SEGMENT
OPC DB 0C3H
_DATA ENDS
_TEXT SEGMENT
START:
        CALL GetCurrentProcessId@0
;в EAX идентификатор текущего процесса
        PUSH EAX
        PUSH 1
;дескриптор может наследоваться
        PUSH PROCESS_VM_OW
;желаемый уровень доступа к процессу
        CALL OpenProcess@12
;в EAX дескриптор открытого процесса
        PUSH 0
;игнорируем параметр
        PUSH 1
;кол-во байт, которые будут записаны
        PUSH OFFSET OPC
;указатель на буфер-источник данных
        PUSH OFFSET RETE
;адрес в памяти процесса, куда собираемся писать
        PUSH EAX
;дескриптор процесса, в память которого мы собираемся
;писать
        CALL WriteProcessMemory@20
;По адресу RETE записывается код C3H. Если это не
;сделать, то будет выполняться бесконечный цикл, и
;программа никогда не закончит свою работу (без
ствий ;извне)

RETE:
        JMP  RETE
        RETN
_TEXT ENDS
END START
```

Модификация сегмента кода с использованием функции VirtualProtectEx. Воспользуемся API-функцией VirtualProtectEx и разрешим доступ к нужным байтам (страницам, на которых располагаются байты), а затем воспользуемся командой MOV: по адресу RETE запишем байт C3H.

```
.586P
.MODEL FLAT,STDCALL
PROCESS_VM_OPERATION  =     0008H
PROCESS_VM_WRITE      =     0020H
PROCESS_VM_OW         =
PROCESS_VM_OPERATION OR PROCESS_VM_WRITE
PAGE_WRITECOPY      = 8
PAGE_EXECUTE              = 10h
includelib "D:\Program Files\Microsoft Visual Studio
.NET\Vc7\PlatformSDK\lib\User32.Lib"
includelib "D:\Program Files\Microsoft Visual Studio
.NET\Vc7\PlatformSDK\lib\Kernel32.Lib"
;импортируемые функции
EXTERN OpenProcess@12:NEAR
EXTERN FlushInstructionCache@12:NEAR
EXTERN VirtualProtectEx@20:NEAR
EXTERN GetCurrentProcessId@0:NEAR
;-------------------------------------------
_DATA SEGMENT
HANDLE  DD ?
NN      DD ?
_DATA ENDS
_TEXT SEGMENT
START:
        CALL GetCurrentProcessId@0
;открыть текущий процесс
        PUSH EAX
        PUSH 1
        PUSH PROCESS_VM_OW
        CALL OpenProcess@12
;разрешить копирование байта по адресу RETE
        MOV  HANDLE,EAX
        PUSH OFFSET NN
;адрес переменной, которая получит старый атрибут
;первой из страниц (если их несколько)
        PUSH PAGE_WRITECOPY
```

```
;устанавливаем атрибут
        PUSH 1
;размер изменяемой области
        PUSH OFFSET RETE
;адрес области памяти, атрибут которой мы будем изменять
        PUSH EAX
;дескриптор процесса, память которого мы модифицируем
        CALL VirtualProtectEx@20
;изменяем байт по адресу RETE
        LEA  EAX,RETE
        MOV  BYTE PTR [EAX],0C3H
;возвращаем байту первоначальный атрибут
        PUSH OFFSET NN
        PUSH PAGE_EXECUTE
        PUSH 1
        PUSH OFFSET RETE
        PUSH HANDLE
        CALL VirtualProtectEx@20
;сбрасываем кэш
        PUSH 1
;размер изменяемой области
        PUSH OFFSET RETE
;адрес области, которую мы изменили
        PUSH HANDLE
;дескриптор процесса, память которого мы изменяем
        CALL FlushInstructionCache@12
;необходимо, чтобы очистить буфер, содержащий команды.
;если этого не сделать, вероятно, что процессор будет
;использовать для выполнения старые команды, "не заметив"
;изменения в памяти
RETE:
        JMP  RETE
        RETN
_TEXT ENDS
END START
```

Успешное выполнение приведенных примеров подтверждает, что модификация кода программы во время ее выполнения в ОС Windows возможна.

Интерактивный дизассемблер и отладчик IDA Pro

IDA Pro (https://www.hex-rays.com) – это интерактивный дизассемблер и отладчик одновременно. Она позволяет превратить бинарный код

программы в ассемблерный текст, который может быть применен для анализа работы программы.

Три кита, на которых держится анализ исполняемого кода в IDA Pro:

- мощное средство анализа исполняемого кода (дизассемблер сам комментирует код и распознает стандартные библиотечные и системные функции), встроенное в дизассемблер. IDA Pro никогда не делает слишком «самоуверенных» предположений. Привилегия на эвристический анализ предоставляется пользователю;
- пользователю предоставляется возможность участвовать в этом анализе, уточнять параметры тех или иных объектов программы, делать исправления;
- наличие библиотеки для написания собственных плагинов (IDA SDK) и встроенный язык программирования (скриптовый язык IDC), весьма близкий по своей структуре к классическому языку C, позволяют значительно наращивать функциональность данного продукта.

IDA используется для анализа вирусов (antivirus companies), исследования защит систем (software security auditing), обратной инженерии (reverse engineering). Хотя IDA и не является декомпилятором (decompiler), она содержит отладчик (debugger) и может анализировать программы на высоком уровне [3].

Реализация

Основываясь на том факте, что модификация кода во время выполнения не препятствует трассировке и что для отладчика она полностью прозрачна, к интерактивному дизассемблеру IDA Pro был написан плагин [4] для проверки наличия модификации сегмента кода в программе во время ее выполнения.

Основными критериями при работе плагина являются: изменение атрибутов сегмента кода во время выполнения программы и наличие функций, способных произвести запись в память процесса.

Для реализации поставленной задачи был применен метод перехвата вызовов API-функций, работающих с атрибутами сегментов, и API-функций, позволяющих произвести запись в память процесса.

Особенности работы плагина

Для хранения истории изменений атрибутов сегмента кода была создана следующая структура:

```
struct about_seg_struct {
    char seg_name[MAXSTR];              // Имя сегмента
    int seg_attr[NUM_CHANGE_ATTR];  // Атрибуты
```

```
                                        // сегмента
    int attr_counter;                   // Счетчик изменений
    int seg_type;                       // Тип сегмента
    bool change_flag;                   // Флаг изменений
    ea_t seg_addr_start;                // Адрес начала сегмента
    ea_t seg_addr_end;                  // Адрес завершения
                                        // сегмента
};
```

При запуске плагина в эту структуру заносятся начальные значения атрибутов. Этот процесс отражен в следующем коде:

```
// Получаем число сегментов
 num_segments = get_segm_qty();
// В цикле проходим через все сегменты и сохраняем их
// начальные атрибуты
 for (int i = 0; i < num_segments; i++)
 {
char segName[MAXSTR];
segment_t *seg = getnseg(i);
    // Получаем имя сегмента
    get_segm_name(seg, segName, sizeof(segName)-1);
    qstrncpy(normal_seg_attr[i].seg_name, segName, MAXSTR);

normal_seg_attr[i].seg_type = seg->type;
    normal_seg_attr[i].seg_attr[0] = seg->perm;
    normal_seg_attr[i].seg_addr_start = seg->startEA;
    normal_seg_attr[i].seg_addr_end = seg->endEA;
    normal_seg_attr[i].func_flag[0] = true;
normal_seg_attr[i].attr_counter = 1;
    normal_seg_attr[i].change_flag = false;
}
```

Дальнейшая работа плагина основана на перехвате вызовов API-функций. Рассмотрим алгоритм, используемый в плагине, для анализа перехваченных функций:

1) если перехвачен вызов API-функции VirtualProtect(Ex) (см. Пример анализа перехваченной функции) – получаем из стека аргументы, переданные функции в момент ее вызова: устанавливаемый атрибут, адрес области памяти, атрибут которой планируется изменять и размер изменяемой области;

2) если перехвачен вызов API-функции WriteProcessMemory – получаем из стека аргументы, переданные функции в момент ее вызова: адрес в памяти процесса, куда намеревались писать, количество байтов, которое планировалось записать.

Решение о наличии или отсутствии модификации кода в программе принимается на основании истории изменения атрибутов сегментов. Процесс проверки изменения атрибутов представлен в следующем коде:

```
// В цикле проходим через все сегменты
for(int i = 0; i < num_segments; i++)
{
// В цикле проходим по всем изменениям в сегменте
 for(int j = 0; j < normal_seg_attr[i].attr_counter; j++)
 {
  // Сравниваем атрибуты
  if((normal_seg_attr[i].seg_attr[j]==0x04)||
     (normal_seg_attr[i].seg_attr[j] == 0x08))
     start_flag = true;

if(start_flag&&((normal_seg_attr[i].seg_attr[j]==0x10)||
      (normal_seg_attr[i].seg_attr[j] == 0x20)))
        {
// Записываем сведения о наличии модификации в файл
        char str_error[MAXSTR];
qsnprintf(str_error,sizeof(str_error)-1,"Change attribute in segment
<%s> and type <%d>!\n", nor-
mal_seg_attr[i].seg_name,normal_seg_attr[i].seg_type);
        ewrite(fp2, str_error, strlen(str_error));
        }
        if((normal_seg_attr[i].seg_attr[j]==0x40)||
 (normal_seg_attr[i].seg_attr[j] == 0x80))
          {
          // Записываем сведения о наличии модификации в файл
char str_error[MAXSTR];
qsnprintf(str_error,sizeof(str_error)-1,"Change attribute in segment
<%s> and type <%d>!\n", nor-
mal_seg_attr[i].seg_name,normal_seg_attr[i].seg_type);
          ewrite(fp2, str_error, strlen(str_error));
          //
          }
        }
        start_flag = false;
        }
```

Правила компиляции плагина

Для создания проекта и компиляции плагина можно воспользоваться средой разработки MS Visual Studio 2005 либо ее более ранними версиями.

Рассмотрим процесс настройки окружения в этой среде:

1. Переходим **File->New->Project…** (Ctrl-Shift-N)
2. Разворачиваем каталог **Visual C++ Projects**, переходим в подкаталог **Win32** и затем выбираем **Win32 Project**. Задаем любое понравившееся имя проекта и нажимаем OK.
3. Далее появится Win32 Application Wizard, нажимаем **Application Settings** и выбираем **Windows Application**, затем выбираем **Empty Project**. Нажимаем **Finish**.
4. В **Solutions Explorer** переходим в каталог **Source Files** и выбираем

Add->Add New Item...

5. Выбираем **C++ File (.cpp)** и подходящее имя файла. Нажимаем **Open**.
6. Переходим в Project->имя_проекта Properties...
7. Выбираем следующие настройки:

Configuration Properties->General: выбираем Configuration Type Динамическая Библиотека (.dll)

C/C++->General: Detect 64-bit Portability Issue отмечаем No

C/C++->General: устанавливаем Debug Information Format в Disabled

C/C++->General: в **Additional Include** добавляем путь к каталогу SDK include, например, C:\IDA\SDK\Include

C/C++->Preprocessor: добавляем __NT__;__IDP__ к Preprocessor Definitions C/C++->Code Generation: отключаем Buffer Security Check и Basic Runtime Checks, устанавливаем Runtime Library в Single Threaded

C/C++->Advanced: устанавливаем __stdcall

Linker->General: выбираем **Output File**, заменяем a .exe на a .plw

Linker->General: добавляем путь к libvc.wXX в **Additional Library Directories**, например, C:\IDA\SDK\libvc.w32

Linker->Input: добавляем ida.lib в Aditional Dependencies

Linker->Debugging: отмечаем No в Generate Debug Info

Linker->Command Line: добавляем /EXPORT:PLUGIN

Build Events->Post-Build Event: устанавливаем Command-line в idag.exe. Нажимаем OK.

Установка плагина

Для загрузки плагина в IDA необходимо скомпилированный .plw файл поместить в каталог plugins. При каждом запуске IDA сканирует этот каталог и загружает плагины.

Руководство по запуску плагина

Запуск плагина осуществляется из меню Edit->Plugins->SMCTracer 4.0 (рис. 2.19).

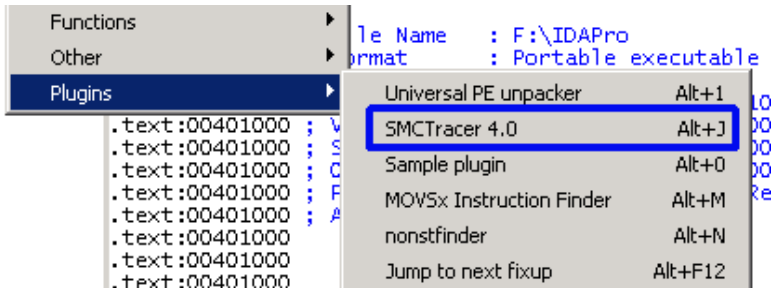


Рис. 2.19. Меню загрузки плагина в IDA Pro

Далее, необходимо указать путь к файлу результатов проверки (рис. 2.20).

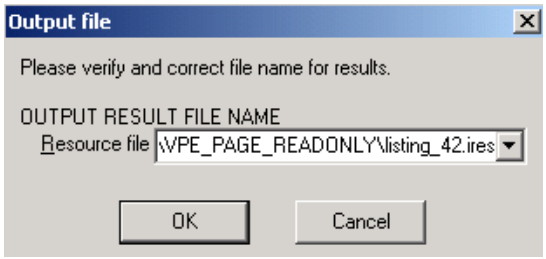


Рис. 2.20. Окно задания имени файла с результатами проверки

Результаты работы плагина

Тестирование плагина проводилось на примерах, рассмотренных в разделе «Примеры модификации сегмента кода во время выполнения программы в ОС MS Windows». Результаты работы плагина следующие:

1) запуск плагина для программы, в которой присутствует модификация сегмента кода с использованием функции WriteProcessMemory

```
Detection a call WriteProcessMemory
(return address: 00401023),
write data to address: 00401023, size of data: 1
WriteProcessMemory write data in segment: <.text>,
at 401000 to 401200
with permission: <Read and Exec>
and type: <Code segment>
```

2) запуск плагина для программы, в которой присутствует модификация сегмента кода с использованием функции VirtualProtectEx

Detection a Call VirtualProtectEx
(return address: 00401028),
new attribute: PAGE_WRITECOPY,
address of modification: 0040105C, size of data: 1
Change attribute in segment 21 is named _**text** permission 8 type 2, function 1 counter 1

Из полученных результатов видно, что созданный плагин сумел обнаружить вызовы API-функций: WriteProcessMemory и VirtualProtectEx. Помимо факта о наличии вызова функции WriteProcessMemory, плагину удалось узнать сегмент, в который происходит запись, тип сегмента и его атрибуты. Для функции VirtualProtectEx плагин указал сегмент, атрибут которого изменяется, и новый атрибут для этого сегмента.

Пример анализа перехваченной функции

Рассмотрим пример анализа перехваченной функции:

```
if(ea == gpa_vp)
{
  // Перехвачен вызов API-функции VirtualProtect
  //
  regval_t rv;
  // Пробуем узнать значение регистра ESP
  // (адрес возврата из функции VirtualProtect)
  if (get_reg_val("esp", &rv))
  {
   ea_t esp = rv.ival;
   invalidate_dbgmem_contents(esp, 1024);
   //
   // Теперь ret_vp содержит значение регистра ESP
   //
   ret_vp = get_long(esp);
   //
   // Из стека “вытаскиваем” параметры, с которыми
   // вызвана функция VirtualProtect:
   // указатель на базовый адрес страницы
   ea_t nameaddr_4 = get_long(esp+4);
   // размер области, атрибут которой изменяется
   ea_t nameaddr_8 = get_long(esp+8);
   // новый атрибут
   ea_t nameaddr_12 = get_long(esp+12);
   // выходной параметр
```

```
  ea_t nameaddr_16 = get_long(esp+16);
  //
  // Сохраняем результаты вызова VirtualProtect в файл
  //
  char log_api_buf[MAXSTR];
  qsnprintf(log_api_buf, sizeof(log_api_buf)-1, "Detection a
  Call VirtualProtect (return address: 00%a), change
  attribut: %s, address of modification: 00%a, size of data:
  %a\n",      ret_vp,      AttrVPEName(nameaddr_12),      nameaddr_4,
nameaddr_12);
  ewrite(fp1, log_api_buf, strlen(log_api_buf));
  //
  // Определяем сегмент, атрибут которого изменился:
  // получаем дескриптор сегмента по адресу
  //
  segment_t* seg_vp = getseg(nameaddr_4);
  if (seg_vp)
  {
   char segName[MAXSTR];
   // Получаем имя сегмента по дескриптору
   get_segm_name(seg_vp, segName, MAXSTR);
   // Следим, чтобы длина, переданная VirtualProtect
   // в качестве параметра, не перекрывала сегменты
   //
   for (int j = 0; j <= nameaddr_8; j++)
   {
    for (int i = 0; i < num_segments; i++)
    {
    //
    // Поверяем, изменился ли атрибут сегмента
    //
     if((normal_seg_attr[i].seg_addr_start<=nameaddr_4+j)    &&    (nor-
mal_seg_attr[i].seg_addr_end>=nameaddr_4+j) &&
(!normal_seg_attr[i].change_flag))
{
    //
    // Запоминаем новый атрибут и устанавливаем флаг
    //
 normal_seg_attr[i].change_flag = true;
 normal_seg_attr[i].seg_attr[normal_seg_attr[i].
 attr_counter] = nameaddr_12;
    //
```

```
    // Записываем результат в файл
    //
 char str43[MAXSTR];
 qsnprintf(str43, sizeof(str43)-1, "Change attr
 in segment %d is named %s permission %d type %d, func
 %d counter %d\n",
 i,                                                    nor-
mal_seg_attr[i].seg_name,                             nor-
mal_seg_attr[i].seg_attr[normal_seg_attr[i.
 attr_counter],
 normal_seg_attr[i].seg_type,
 normal_seg_attr[i].func_flag[normal_seg_attr[i].
 attr_counter],
 normal_seg_attr[i].attr_counter);
 ewrite(fp1, str43, strlen(str43));
    //
    // Увеличиваем счетчик числа изменений
    //
normal_seg_attr[i].attr_counter++;                      }

      }
    }
  }

  // Получаем имя сегмента, из которого была вызвана
  // VirtualProtect
  char segName[MAXSTR];
  segment_t *seg = getseg(ret_vp);
  //
  // Проверяем дескриптор сегмента
  //
  if(seg)
  {
    char perm_seg_buf[MAXSTR];
    get_true_segm_name(seg, segName, MAXSTR);

  // Записываем результат в файл
    qsnprintf(perm_seg_buf, sizeof(perm_seg_buf)-1, "Segment
    for return address: <%s>, at %a to %a with permission:
    <%s> and    type: <%s> \n\n", segName, seg->startEA, seg
    ->endEA, SegPermName(seg->perm), SegTypeName(seg->type));
    ewrite(fp1, perm_seg_buf, strlen(perm_seg_buf));
```

```
  }
  // Продолжаем процесс отладки программы
  continue_process();
 }
 else
 {
  // Если функция получения содержимого регистра
  // вернула ошибку
  msg("Error! in get_reg_val(esp)\n");
  clear_requests_queue();
  request_exit_process();
  run_requests();
 }
}
```

В результате проделанной работы к интерактивному дизассемблеру IDA Pro был создан плагин. Данный продукт, путем автоматизированной отладки, способен обнаруживать признаки наличия модификации сегмента кода во время выполнения программы.

Сведения, полученные в результате работы плагина применимы при исследованиях компьютерных вирусов, защитных механизмов, сетевых червей и прочих программ, которые используют модификацию сегмента кода во время своего выполнения.

Благодаря огромным возможностям IDA, функциональность созданного плагина легко расширить. В качестве наиболее перспективных направлений расширения возможностей плагина можно выделить следующие:

- обнаружение модификации сегмента данных и стека во время выполнения программы,
- объединение статических и динамических возможностей IDA в единое статическо-динамическое средство обнаружения модификации кода. Таким образом, попытаться разрешить проблему построения полного алгоритма при динамическом исследовании программы.

Библиографический список

1. *Пирогов В.Ю.* Ассемблер и дизассемблирование. – СПб.: БХВ-Петербург, 2006. – 464 с.
2. *Касперски К.* Компьютерные вирусы изнутри и снаружи. – СПб.: Питер, 2006. – 522 с.
3. *Касперски К.* Фундаментальные основы хакерства. Искусство дизассемблирования. – М.: СОЛОН-Пресс, 2005. – 448 с.

4. *Micallef Steve*. IDA PLUG-IN WRITING IN C/C++, 2009 [Электронный ресурс]. – URL: http://www.binarypool.com/ idapluginwriting/idapw.pdf (дата обращения: 02.11.2015).

2.6. Технология PLC (Power Line Communication) как потенциальный технический канал утечки информации

В настоящее время можно столкнуться с точкой зрения, что «…тысячи и тысячи организаций по сей день, вместо того чтобы вкладывать деньги в развитие и модернизацию оборудования, обязаны покупать и устанавливать на рабочих местах, оснащенных СВТ, сетевые фильтры – достаточно дорогое и, как представляется, абсолютно бесполезное для них и очень прибыльное для производителей этих “игрушек” “удовольствие”. К категории бесполезных с точки зрения защиты информации средств следует отнести и генераторы шума, установка которых необходима по требованию ФСТЭК России на всех рабочих местах, где осуществляется обработка служебной информации ограниченного распространения и информации, составляющей государственную тайну. Компьютеры, побочные электромагнитные излучения и наводки которых позволили бы снять информацию за пределами рабочего места оператора, уже практически не производятся, а требование об обязательной установке сетевого фильтра и/или генератора шума остается» [1].

Не желая спорить с автором по его позиции относительно средств защиты, задаешься вопросом, часто ли, по факту, производится детальная проверка того, что входит в состав вспомогательных технических средств и систем (ВТСС) – технических средств и систем, непосредственно не участвующих в обработке конфиденциальной информации, но использующихся совместно с ТСПИ и находящихся в зоне создаваемого ими электромагнитного поля, например, таких как настольные лампы, электронные часы, обогреватели, тройники и т. п., подключаемые к сети переменного напряжения 220В/50Гц? Зачастую присутствия таких устройств в контролируемой зоне быть не должно, но по факту «временно», для решения каких-либо сиюминутных задач, они, тем не менее, используются.

Исходя из вышесказанного, хотелось бы обратить внимание на возможности технологии PLC (Power Line Communication) и приборы на ее основе.

Технология PLC (Power Line Communication) – телекоммуникационная технология, базирующаяся на использовании силовых электросетей для высокоскоростного информационного обмена. Эксперименты по передаче данных по электросети велись достаточно давно, но низкая скорость передачи и слабая помехозащищенность были наиболее узким ме-

стом данной технологии. Но прогресс не стоит на месте, и появление более мощных современных энергоэффективных DSP-процессоров (цифровые сигнальные процессоры) дали возможность использовать более сложные способы модуляции сигнала, такие как OFDM модуляция (Orthogonal Frequency Division Multiplexing), что позволило значительно продвинуться вперед в реализации технологии PLC.

Несколько лет назад несколько крупных лидеров на рынке телекоммуникаций объединились в альянс, получивший название HomePlug Alliance, с целью совместного проведения научных исследований и практических испытаний, а также принятия единого стандарта на передачу данных по системам электропитания. Прототипом PowerLine является технология PowerPacket фирмы Intellon, положенная в основу для создания единого стандарта HomePlug1.0 specification (принят альянсом HomePlug 26 июня 2001 г.), в котором определена скорость передачи данных до 14 Мб/с.

Одним из применений данной технологии было решение задачи последней мили Интернета, особенно в США, где традиционно преобладают внутридомовые сети электропитания 120В/60Гц. Из-за вдвое меньшего напряжения в сети вдвое увеличивается токовая нагрузка (и в четыре раза потери на нагрев проводов при равном сопротивлении) при тех же значениях потребляемой мощности, в связи с чем понижающие трансформаторные подстанции располагаются в непосредственной близости от потребителя, что способствовало продвижению этой технологии.

PowerLine технология может быть использована при создании локальной сети в небольших офисах (до 10 компьютеров), где основными требованиями к сети являются простота реализации, мобильность устройств и легкая расширяемость. При этом как вся офисная сеть, так и отдельные ее сегменты могут быть построены с помощью PowerLine адаптеров.

Основой технологии Powerline является использование частотного разделения сигнала, при котором высокоскоростной поток данных разбивается на несколько относительно низкоскоростных потоков, каждый из которых передается на отдельной поднесущей частоте с последующим их объединением в один сигнал – метод ортогонального частотно-разделенного мультиплексирования (OFDM). При этом центры поднесущих частот размещены так, что пик каждого последующего сигнала совпадает с нулевым значением предыдущих. Такое размещение позволяет более эффективно использовать доступную полосу частот.

Теоретическая скорость передачи данных при использовании параллельных потоков с одновременным фазовым модулированием сигналов составляет более 100 Мб/с. При передаче сигналов по бытовой сети электропитания могут возникать большие затухания в передающей функции

на определенных частотах, что может привести к потере данных. В технологии Powerline предусмотрен специальный метод решения этой проблемы – динамическое выключение и включение передачи сигнала (dynamically turning off and on data-carrying signals). Суть данного метода заключается в том, что устройство осуществляет постоянный мониторинг канала передачи с целью выявления участка спектра с превышением определенного порогового значения затухания. В случае обнаружения данного факта использование этих частот на время прекращается до восстановления нормального значения затухания. Данный метод делает технологию Powerline максимально гибкой при использовании в различных условиях. Например, в разных странах существуют различные регулирующие правила, согласно которым часть диапазона частот не может быть использована. При этом, в случае Powerline, в этом диапазоне просто не будут передаваться данные.

В Powerline используется двухступенчатое (каскадное) помехоустойчивое кодирование битовых потоков перед тем, как они будут промодулированы и поступят в канал передачи данных. Суть помехоустойчивого кодирования состоит в добавлении в исходный информационный поток по определенным алгоритмам избыточных («защитных») битов, которые используются декодером на приемном конце для обнаружения и исправления ошибок. Каскадирование блочного кода Рида–Соломона и простого сверточного кода, декодируемого по алгоритму Витерби, позволяет исправлять не только одиночные ошибки, но и пакеты ошибок, обеспечивая тем самым практически 100% гарантию целостности передаваемых данных. Кроме того, помехоустойчивое кодирование является и способом технического закрытия, обеспечивающего относительную безопасность передаваемой информации в общей среде передачи.

В качестве решения проблемы того, что сеть бытового электропитания служит общей средой передачи данных, т. е. в один момент времени передачу могут осуществлять сразу несколько устройств. В такой ситуации для разрешения конфликтов столкновения трафика необходим регулирующий механизм – протокол доступа к среде. В качестве такого протокола был выбран хорошо известный Ethernet, который в технологии Powerline был расширен путем добавления дополнительных полей приоритезации. Такая модификация вызвана необходимостью гарантированной полосы пропускания для передачи голоса и видео через IP, когда величина задержки является критичным параметром. Пакеты, содержащие голос или видео, в этом случае помечаются как «timing critical», т. е. имеют самый высокий приоритет при обработке и доступе к среде передачи. Возможна работа устройств Powerline и в зданиях с разнофазным током, но при значительном снижении производительности сети. В современных устройствах HomePlug AV реализовано 128-битное шифрование AES.

На данный момент производится множество устройств PLC HomePlug AV, реализующих функцию Ethernet моста (Powerline D-Link DHP-600AV; Powerline TP-LINK TL-PA4010KIT; Powerline UPVEL UA-251P), в том числе, с поддержкой PoE (Powerline Zyxel PLA4201v2 EE) со скоростью передачи данных от 200 до 600 Мбит/с и дальностью 100–300 м. В сочетании с уже выпускаемыми изделиями обеспечивающими передачу аудио- и видеоданных, например, камерой PLANET ICA-1200 Cube IP (PoE, ИК подсветка, изображение высокой четкости для круглосуточного IP видеонаблюдения, форматы H.264, MPEG-4 и JPEG Full HD разрешение, до 30 кадров в секунду), имеем уже готовый промышленно производимый комплект «кубиков» для построения системы дистанционного наблюдения.

В ближайшее время ожидается появление чипа, позволяющего встраивать его в различные приборы, которые будут иметь возможность принимать и передавать данные через собственные цепи питания. С помощью данного чипа можно организовать передачу аудио- и видеоданных, данных с датчиков охранной сигнализации, расширять и продлять телефонные линии, и… реализовать решение задачи по дистанционному, возможно несанкционированному, сбору и передаче данных от соответствующего вида приемных устройств. Причем, при ухудшении условий передачи данных (большая длина линии, шумящие приборы, подключенные к сети), при снижении скорости до 50 раз относительно максимального значения (до 10 Мбит), может сохраняться приемлемое функционирование технического канала утечки информации (однозначно для аудиопотока и при наличии достаточно эффективного кодека умеренного разрешения – для видеопотока). Как говорится, комментарии излишни.

Существуют некоторые признаки, которые позволяют обнаружить оборудование на основе технологии PLC HomePlug AV, по крайней мере, в настоящий момент: повышенный уровень тепловыделения для непрерывно работающего в активном режиме прибора (минимум 3,5 Вт), характерный уровень и вид сигнала в линии электропитания. В связи с чем долговременное функционирование технического канала утечки информации на основе технологии PLC HomePlug AV без его обнаружения маловероятно, однако возможно эпизодическое возникновение утечек, в том числе по расписанию, либо по активации внешним сигналом.

В связи с чем установка на рабочих местах, оснащенных СВТ, сетевых фильтров, генераторов шума, в том числе по сетям электропитания, в соответствии с требованиями ФСТЭК России – не надуманное требование. Отчасти, это одна из упреждающих мер по противодействию подобным устройствам.

Библиографический список

1. *Атаманов Г.А.* Технические каналы утечки информации: определение, сущность, классификация // Защита информации. Инсайд. – 2010. – № 1. – С. 2-7.
2. Технология PLC (Power Line Communication) [Электронный ресурс]. – URL: http://network.xsp.ru/5_5.php (дата обращения: 12.09.2015).
3. Интернет из розетки: общие принципы работы технологии и обзор Powerline-адаптера TP-LINK TL-PA6010 [Электронный ресурс]. – URL: http://www.3dnews.ru/821880 (дата обращения: 12.09.2015).
4. NetGear Support Главная страница службы поддержки / Часто задаваемые вопросы по адаптерам Powerline [Электронный ресурс]. – URL: http://kb.netgear.ru/ (дата обращения: 12.09.2015).

Глава 3. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Криптографическая защита сетевых технологий

Шифрование является основным средством обеспечения конфиденциальности передаваемых по каналам связи данных. Криптографическая защита каналов передачи данных может быть реализована на следующих уровнях, для каждого из которых характерно использование определенных средств защиты и протоколов:

- физический уровень – специфической формой шифрования, реализуемой аппаратно и применимой только на физическом уровне, является защита передачи (защита по ширине частотного спектра);
- сетевой уровень – шифрование передаваемого между узлами трафика (например, протокол IPSec);
- уровень представления – шифрование данных, передаваемых между удаленными приложениями (например, протоколы SSL и TLS);
- прикладной уровень – самостоятельное шифрование данных приложениями.

Кроме того, криптографические методы и средства могут использоваться для решения задач аутентификации сторон информационного обмена, обеспечения аутентичности и неотрекаемости источника данных и целостности передаваемых данных.

Вопросы информационной безопасности распределенных систем (сетей) достаточно полно и глубоко трактуются в технической спецификации X.800 Международного союза электросвязи [1], при этом шифрование и цифровая подпись рассматриваются в качестве ключевых механизмов безопасности. Данный документ лег в основу стандарта ISO 7498-2:1989 и отечественного гармонизированного стандарта ГОСТ Р ИСО 7498-2–1999 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации». Криптографические механизмы могут быть реализованы на разных уровнях эталонной модели взаимодействия сетей OSI, рекомендуемые X.800 уровни реализации приведены в табл. 3.1. На прикладном уровне могут быть обеспечены все услуги безопасности.

На самых нижних уровнях сетевой архитектуры (физическом и канальном) шифруются абсолютно все данные, проходящие по каналу связи, включая открытый текст сообщения и служебную информацию (заголовки, маршрут сообщения, информация об используемом коммуникацион-

ном протоколе). Такой вид шифрования обычно называется *канальным* (link encryption). Не шифруется только трафик управляющих сообщений канального уровня, который включает в себя команды и параметры, используемые различными канальными устройствами для синхронизации процесса коммуникаций. Канальное шифрование весьма эффективно, однако требует раскрытия данных (расшифровывания заголовков для получения служебной информации и повторного шифрования для дальнейшей передачи) в каждом промежуточном узле сети (например, на маршрутизаторе). Эта особенность требует дополнительной защиты всех коммуникационных узлов сети, что может существенно повысить стоимость реализации. Шифрование служебной информации, имеющей типовую структуру, может привести к появлению статистических закономерностей в шифртекстах, может облегчить криптоаналитику задачу определения используемых криптографических ключей. Примером защищенного протокола канального уровня является PPTP, использующийся в технологии VPN-туннелирования компании Microsoft.

Таблица 3.1

Связь между сервисами безопасности и уровнем шифрования (X.800)

Требование	Сервис безопасности	Уровень шифрования
полная конфиденциальность потока трафика	полная конфиденциальность	1 (физический уровень)
высокая градация защиты (наличие потенциально отдельного ключа для каждой ассоциации приложений)	целостность без восстановления, предотвращение отказа от авторства, селективная защита полей, полная конфиденциальность	6 (уровень представления)
массовая защита всей связи между оконечными системами и/или внешними устройствами шифрования	конфиденциальность и целостность без восстановления	3 (сетевой уровень)
целостность с восстановлением вместе с высокой градацией защиты	конфиденциальность и целостность с восстановлением и без восстановления	4 (транспортный уровень)

Шифрование на верхнем уровне сетевой архитектуры (прикладном, уровне представления) обычно называется *сквозным* (end-to-end

encryption). При сквозном шифровании данные остаются зашифрованными, пока не будут доставлены к месту назначения. Шифрование на прикладном уровне более гибко, так как оставляет пользователям (пользовательским приложениям) решение вопроса о необходимости шифрования тех или иных сообщений. С другой стороны, криптоаналитик получает возможность анализа трафика, так как дополнительная информация (о маршрутизации, размере передаваемых сообщений, частоте обмена данными между конкретными абонентами, связи этого обмена с различными внешними событиями) остается открытой. Примером прикладного защищенного протокола является S/MIME, позволяющий пользователям шифровать и подписывать сообщения электронной почты.

Сетевые механизмы безопасности используют как симметричные, так и асимметричные криптосистемы. Обычно асимметричная схема служит для обеспечения аутентификации сторон и распределения сеансовых ключей, симметричные шифры – для непосредственного шифрования передаваемых данных.

Для создания надежной линии передачи сообщений с помощью асимметричной схемы шифрования между отправителем и получателем необходимо создать надежную схему передачи открытых ключей. При непосредственном обмене открытыми ключами возможна реализация классической сетевой атаки «человек посередине» (man in the middle). Подменив передаваемые ключи, злоумышленник-посредник может представить себя как отправителем подписанных данных, так и получателем зашифрованных сообщений.

Поэтому одной из наиболее серьезных проблем при использовании методов криптографии с открытым ключом является проверка, действительно ли открытый ключ принадлежит абоненту, с которым планируется вести обмен зашифрованными сообщениями. Эта проблема решается с помощью методов цифровой сертификации.

Цифровой сертификат – электронный документ, который связывает открытый ключ с определенным пользователем или приложением. Информация сертификата подтверждает истинность открытого ключа и владельца соответствующего личного ключа.

Наиболее распространенным стандартом цифровых сертификатов является X.509, хотя используются сертификаты и других форматов [2].

Функции выдачи, отзыва и управления цифровыми сертификатами берет на себя служба сертификации (удостоверяющий центр, центр сертификации, Certification Authority – CA). Наряду с удостоверяющими центрами государственных структур существуют и коммерческие службы сертификации. Служба сертификации выступает в качестве гаранта истинности связи между открытым ключом субъекта и идентифицирующей этот субъект информацией, т. е. позволяет соотнести открытые ключи с их владельцами.

Для полноценного функционирования сетевых сервисов, базирующихся на асимметричных криптосистемах (например, электронной цифровой подписи), требуется создание развитой инфраструктуры, базирующейся на использовании цифровых сертификатов. Такая структура, позволяющая предоставлять доверенные действительные открытые ключи участников и управлять всем жизненным циклом цифровых сертификатов, получила название PKI (Public Key Infrastructure).

Инфраструктура открытых ключей или **PKI** – полный комплекс программно-аппаратных средств, а также организационно-технических мероприятий, необходимых для использования технологий шифрования с открытыми ключами и ЭЦП. PKI обеспечивает взаимодействие между службой управления сертификатами и конечными пользователями (рис. 3.1). Компонентами инфраструктуры открытых ключей PKI являются [2]:

- удостоверяющий центр – собственно система выдачи и управления цифровыми ключами и сертификатами; выполняет аутентификацию конечных пользователей и подписывает сертификаты перед их распространением;
- регистрирующий центр – не обязателен, может служить в качестве промежуточного звена между удостоверяющим центром и конечными пользователями, снижая нагрузку на удостоверяющий центр; генерирует ключи, принимает и проверяет регистрационную информацию о новых реестрах, принимает и проверяет полномочия запросов на восстановление и резервное копирование ключей, а также на отзыв сертификатов;
- каталог сертификатов – централизованное хранилище сертификатов;
- сервер восстановления ключей – предоставляет удостоверяющему центру возможность создавать резервные копии личных ключей в момент их создания и восстанавливать их в случае необходимости;
- протоколы администрирования – обеспечивают взаимодействие конечных пользователей и службы управления сертификатами (например, взаимодействие регистрирующего центра с конечным пользователем или взаимодействие двух удостоверяющих центров для обеспечения перекрестной сертификации);
- операционные протоколы – определяют структуры данных при передаче сертификатов и информации об отмене сертификатов конечными пользователями, каталогами и доверяющими сторонами.

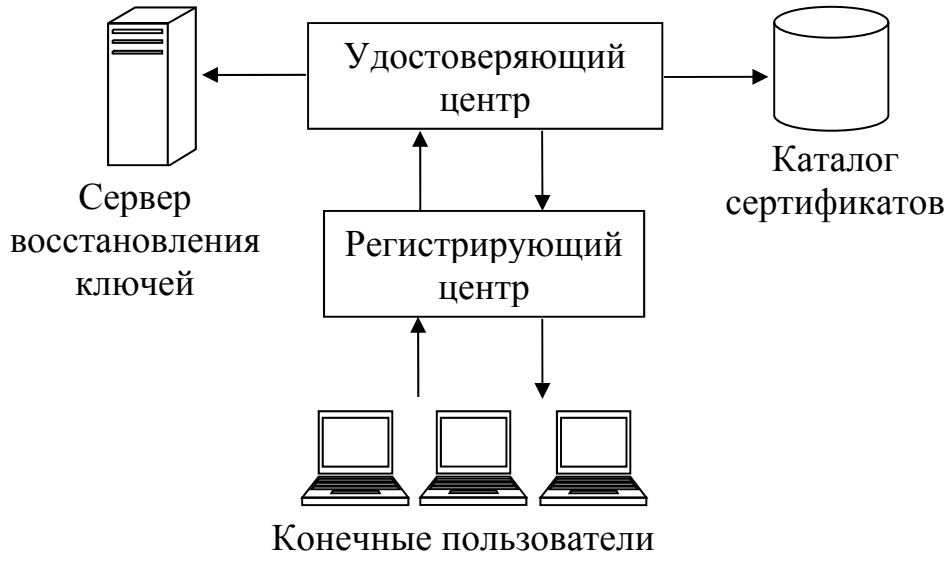


Рис. 3.1. Компоненты инфраструктуры открытых ключей

Далее рассмотрены наиболее известные сетевые протоколы защищенного обмена данными и аутентификации.

Протокол IPSec (IP Security) – набор криптографических протоколов для обеспечения защиты передаваемых данных в IP-сетях. Протокол может функционировать на сетевом или транспортном уровне модели OSI. Использование протокола IPSec является преобладающим в реализациях виртуальных частных сетей (VPN-туннелей), на рынке представлены как программные, так и программно-аппаратные реализации этого протокола.

IPSec определяет [2, 3]:

- протоколы защиты передаваемого потока AH (Authentication Header) и ESP (Encapsulating Security Payload);
- параметры защищенного канала передачи данных SA (Security Associations), характеризующие соединение (например, используемые алгоритм шифрования, хэш-функция, секретные ключи, номер пакета и др.);
- протокол обмена криптографическими ключами IKE (Internet Key Exchange);
- алгоритмы шифрования данных и аутентификации.

Протокол IPSec обеспечивает:

- аутентификацию сторон при создании защищенного канала;
- обеспечение конфиденциальности (шифрование) и целостности передаваемых данных;
- распределение ключей между сторонами.

IPSec не устанавливает обязательной поддержки каких-то определенных алгоритмов шифрования и обеспечения целостности данных, од-

нако спецификация IPSec содержит рекомендованные алгоритмы, использование которых призвано обеспечить совместимость между различными реализациями протокола. Существуют реализации протокола, поддерживающие отечественные стандарты криптографической защиты информации (например, КриптоПро IPSec).

Для шифрования данных используется симметричное шифрование, реализуемое протоколом ESP. Рекомендуемым алгоритмом шифрования является DES в режиме сцепления блоков шифртекста CBC (DES-CBC). Более современные рекомендации IPSec позволяют использовать и другие алгоритмы блочного шифрования (AES, Triple DES, Blowfish, IDEA, 3IDEA, CAST, RC5), если они поддерживаются обеими сторонами взаимодействия. Конкретные криптоалгоритмы могут добавляться производителями, однако практически все современные реализации протокола поддерживают AES-шифрование (AES-CBC и AES-CTR). Кроме шифрования, ESP обеспечивает целостность пакетов, а также защиту от их повторной передачи (рекомендуемые криптографические алгоритмы для вычисления контрольной суммы: HMAC с функцией хэширования SHA-1 или MD5, в настоящее время может использоваться AES-XCBC-MAC). Сервисы аутентификации предоставляются опционально. Для аутентификации пакетов используются хэш-значения (HMAC), а не цифровые подписи. Возможно отключение шифрования или аутентификации (но не обоих одновременно), в этом случае используется соответствующий пустой алгоритм (NULL algorithm).

Протокол AH обеспечивает целостность передаваемых данных и аутентификацию их источника и опционально – защиту от повторной передачи данных. Для вычисления контрольных сумм протокол AH использует те же алгоритмы, что и ESP (обычно HMAC-SHA1 или AES-XCBC-MAC).

Протоколы ESP и AH могут использоваться по отдельности или совместно, определены два режима их работы: *туннельный* и *транспортный*. *Туннельный режим* функционирует на сетевом уровне, подходит для построения виртуальных частных сетей (VPN) и предполагает шифрование всего исходного IP-пакета совместно с его последующей инкапсуляцией. Поскольку IPSec работает на уровне IP-протокола, созданный защищенный канал может использоваться протоколами более высоких уровней, например TCP/UDP или прикладные протоколы. *Транспортный режим* функционирует на более высоком уровне сетевой архитектуры, производится шифрование только данных IP-пакета, исходный заголовок не изменяется. Этот режим подходит для защиты туннелей, организованных другими средствами (например, L2TP).

Протокол IKE обеспечивает начальную аутентификацию сторон, а также распределение ключей. Формирование общего секретного ключа

для сессии производится с использованием алгоритма Диффи–Хеллмана (DH), аутентификация – с помощью цифровых сертификатов сторон (X.509, обычно используется цифровые подписи RSA или ECDSA). Сначала производится согласование параметров SA (защищенного канала), затем формируется общий ключ с помощью системы Диффи–Хеллмана, и лишь затем проводится аутентификация сторон взаимодействия. IPSec допускает возможность установки ключа сессии вручную без использования IKE, однако этот метод не рекомендуется и используется крайне редко.

Протоколы SSL/TLS – протоколы создания защищенного канала связи в клиент-серверных системах (между двумя приложениями, как правило, между клиентом и сервером в сети Интернет). Протоколы SSL/TLS работают поверх протоколов транспортного уровня, например TCP. С другой стороны, они располагаются ниже прикладного уровня и не зависят от используемого прикладного протокола стека TCP/IP, поэтому могут использоваться совместно с любым из них (например, частое использование совместно с протоколом HTTP привело к появлению защищенного прикладного протокола HTTPS). Разные источники относят протоколы SSL/TLS либо к транспортному уровню, либо к уровню представления.

Протокол SSL (Secure Sockets Layer) разработан специально для обеспечения безопасной передачи данных по протоколу HTTP между узлами сети Интернет. Протокол обеспечивает конфиденциальность (за счет симметричного шифрования) и целостность (за счет использования кодов аутентификации) сообщений, а также аутентификацию сервера и необязательную аутентификацию клиента (за счет использования цифровых сертификатов). Протокол SSL поддерживается большинством интернет-браузеров, доминирующей является версия SSL 3.0. В настоящее время протокол SSL признан небезопасным, на его основе разработан более современный протокол TLS (Transport Layer Security), первая версия которого вышла в 1999 г. TLS не обеспечивает совместимости с SSL.

TLS состоит из двух протоколов, имеющих различное назначение:

- TLS Handshake Protocol – установление защищенного сеанса связи, взаимная аутентификация приложений и безопасный обмен криптографическими ключами;
- TLS Record Protocol – обеспечение конфиденциальности и целостности передаваемых данных.

TLS Handshake Protocol предусматривает согласование используемых криптографических алгоритмов (шифрования и хэширования), обмен сеансовыми случайными величинами и криптографическими параметрами для дальнейшего формирования ключей, обмен и проверку сертификатов (X.509) для аутентификации сторон (или только сервера), формирование общего сеансового ключа, проверку предыдущих этапов подтверждения

связи (с помощью HMAC с MD5, SHA-1 или SHA-2). Сеансовый ключ передается в зашифрованном виде (с помощью асимметричной криптосистемы RSA), либо формируется по алгоритму Диффи–Хеллмана. Поддерживаются цифровые подписи RSA, DSA, ECDSA и хэш-функции MD5, SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512).

TLS Record Protocol использует параметры, полученные во время работы TLS Handshake Protocol. Он реализует симметричное шифрование, сжатие и проверку целостности передаваемых данных. Доступные для использования алгоритмы определяются версией протокола TLS. Симметричные блочные шифры используются в режиме сцепления блоков шифртекста CBC. В текущей версии TLS 1.2 доступны: AES (128, 256), Triple DES и потоковый шифр RC4. Каждое сообщение снабжается кодом аутентификации HMAC (с MD5, SHA-1 или SHA-2). Использование шифрования и/или кодов аутентификации может быть отключено.

Протоколы SSL/TLS позволяют создать VPN-туннель в интернет-соединениях и приложениях электронной коммерции, обеспечивая безопасность не только HTTP, но и других прикладных протоколов, таких как SMTP, FTP. Протоколы поддерживаются большинством современных браузеров и операционных систем на разных платформах, имеют программные и аппаратные реализации. Существуют реализации протокола TLS с поддержкой российских криптографических стандартов (например, КриптоПро TLS, входящий в состав КриптоПро CSP, реализация TLS в составе Валидата CSP, ViPNet CSP, Континент TLS VPN и др.).

Протокол Kerberos – протокол взаимной аутентификации и распределения сеансовых ключей в клиент-серверных системах с участием третьей (доверенной) стороны [3, 4]. Kerberos является одной из модификаций протокола взаимной аутентификации Нидхема–Шредера с применением симметричных криптосистем.

В качестве симметричных шифров могут быть использованы DES, 3DES и AES в режиме CBC. К передаваемым данным перед шифрованием добавляется контрольная сумма, в роли которой могут выступать коды аутентификации HMAC (с хэш-функциями MD4, MD5, SHA-1), хэш-значения или контрольная сумма CRC-32. Доверенной стороной выбираются наиболее стойкие криптографические алгоритмы из списка тех, которые поддерживаются сторонами.

При непосредственной аутентификации на сервере пользователь вынужден проходить процедуру для каждой службы сети, а каждый сервер – хранить ключи и регистрационную информацию всех клиентов. Такая система не слишком удобна для пользователей и создает дополнительные риски безопасности. Протокол Kerberos предполагает *централизованное хранение аутентификационной информации* клиентов и позволяет реализовать *принцип единого входа* (Single Sign-On) – возможность использова-

ния единой учетной записи пользователя для доступа к любым службам и ресурсам сети без повторной аутентификации. Протокол Kerberos и его расширение, позволяющее проводить аутентификацию с помощью цифровых сертификатов, реализован в операционных системах Windows Server.

Kerberos обеспечивает аутентификацию в недоверенной среде, подразумевающей наличие у противника следующих возможностей:

- способность выдать себя за одну из сторон сетевого взаимодействия;
- физический доступ к одному из участвующих в соединении компьютеров;
- перехват, модификация и повторная передача пакетов.

Безопасность протокола Kerberos требует обязательной синхронизации системных часов всех участвующих во взаимодействии узлов.

В роли *доверенной стороны* (арбитра) выступает служба KDC (центр распределения ключей, Kerberos Key Distribution Center), работающая на физически защищенном сервере. В сетях под управлением операционной системы Windows Server KDC располагается на контроллере домена. KDC хранит базу регистрационных данных всех клиентов сети, а также секретные ключи клиентов, используемые для шифрования служебной информации, передаваемой в процессе аутентификации. Эти ключи, называемые долговременными, используются пользователями только для связи с KDC. Предполагается, что секретный ключ известен обеим сторонам (и клиенту, и KDC) и был передан надежным способом до начала взаимодействия.

В состав службы KDC входят сервер аутентификации AS (Authentication Server) и служба выдачи разрешений TGS (Ticket Granting Service, Ticket Granting Server).

Основными элементами безопасности Kerberos являются *билеты* (мандаты, ticket) и *аутентификаторы* (authenticator). Билеты предназначены для безопасной передачи серверу личности клиента и имеют определенный политикой безопасности срок действия (обычно не более 8 часов). Аутентификатор – это дополнительный одноразовый атрибут, предъявляемый вместе с билетом. Особенностью протокола Kerberos является использование концепции TGT (ticket granting ticket, билет для получения билета), позволяющей клиентам однократно пройти аутентификацию для доступа к нескольким сервисам в течение определенного времени.

Пусть клиент A хочет получить доступ к сетевому сервису на сервере SS (Service Server). Тогда, в несколько упрощенном виде, участники протокола Kerberos должны будут выполнить следующие шаги (рис. 3.2).

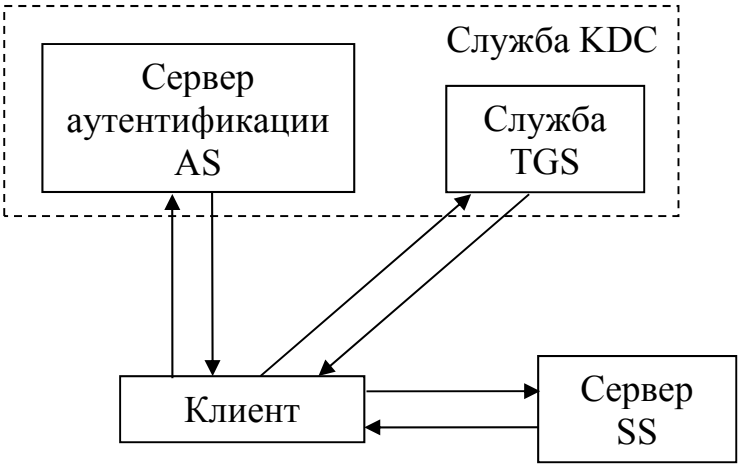


Рис. 3.2. Аутентификация Kerberos

1. Клиент A отсылает серверу аутентификации AS запрос, содержащий идентификатор клиента (A), идентификатор сервиса (SS) и метку времени клиента T_A, зашифрованную долговременным ключом клиента.

   A: $\{A, SS, E_A(T_A)\} \rightarrow AS$,

   где E_A – симметричный шифр на долговременном ключе клиента A.
2. Сервер аутентификации AS проверяет наличие регистрационных данных клиента A в базе данных учетных записей и проводит первоначальную аутентификацию клиента по знанию секретного ключа. Если клиент зарегистрирован и при расшифровании сервером AS получена правильная метка времени, AS предоставляет клиенту информацию для доступа к серверу выдачи разрешений. Клиенту A направляются:
   - идентификатор сервера TGS (обозначим его ITGS) и случайный сеансовый ключ K_1 для связи A с TGS, зашифрованные секретным ключом клиента A;
   - билет TGT, зашифрованный ключом сервера TGS;
   - срок действия L билета TGT (время начала и окончания действия) и сгенерированная сервером аутентификации метка времени T_{AS}.

   TGT содержит копию сеансового ключа для связи с A, срок действия билета, метку времени и идентификатор клиента.

   AS: $\{E_A(ITGS, L, K_1, T_{AS}), TGT\} \rightarrow A$,

   где $TGT = E_{TGS}(A, L, K_1, T_{AS})$, E_{TGS} – симметричный шифр на секретном ключе сервера TGS.
3. Получив сообщение, клиент расшифровывает свою часть с целью получения сеансового ключа K_1 для связи с сервером TGS. Клиент пересылает TGT службе TGS. Кроме того, он отсылает свой аутентификатор, зашифрованный сеансовым ключом K_1, и идентификатор сервиса SS. Аутентификатор содержит идентификатор клиента и новую метку времени T_A.

A: {TGT, SS, E_{K1}(A, T_A)} → TGS

4. Служба TGS расшифровывает полученный от клиента TGT, теперь она имеет в своем распоряжении ключ K_1 и может расшифровать остальные присланные клиентом данные. В ответ служба TGS генерирует билет сервиса (TGS, service ticket) и шифрует его секретным ключом сервера SS. Билет сервиса включает: идентификатор клиента, случайный сеансовый ключ K_2 для связи клиента A с сервисом SS, время жизни билета и метку времени. Кроме того, служба TGS направляет пользователю копию сеансового ключа, идентификатор сервиса и время жизни билета L, зашифрованные ключом K_1.

   TGS: {E_{K1}(SS, K_2, L), TGS} → A,

   где TGS = E_{SS}(A, L, K_2, T_{TGS}), E_{SS} – симметричный шифр на секретном ключе сервера SS. Служба TGS является таким же сетевым сервисом, как и остальные, поэтому билеты TGT и TGS имеют одинаковую структуру.
5. Клиент A расшифровывает свою часть сообщения и получает сеансовый ключ для связи с сервером SS. Теперь A может пройти авторизацию на сервисе. A посылает серверу SS полученный билет сервиса и новый аутентификатор (идентификатор клиента и его метку времени), зашифрованный на сеансовом ключе K_2, предназначенном для связи клиента A с сервером SS.

   A: {TGS, E_{K2}(A, T_A)} → SS
6. Сервер SS расшифровывает билет сервиса своим секретным ключом и извлекает сеансовый ключ K_2 для связи с клиентом A. Теперь он может расшифровать присланный клиентом аутентификатор. Сервер SS подтверждает свою подлинность клиенту, посылая ему значение $T_A + 1$, зашифрованное общим ключом K_2.

   SS: $E_{K2}(T_A + 1)$ → A
7. Клиент расшифровывает сообщение и проверяет корректность обновления своей метки времени. Если время обновлено корректно, пользователь может доверять серверу.

При необходимости общий сеансовый ключ K_2 может использоваться для дальнейшего шифрования сообщений между клиентом A и сервером SS.

Если требуется односторонняя аутентификация только клиента серверу, шаги 6–7 опускаются.

Kerberos может использоваться и для междоменной аутентификации. В случае обращения клиента к серверу из другого домена KDC выдает билет переадресации для обращения к KDC другого домена. Это предполагает наличие ключей для взаимной связи KDC разных доменов.

Использование в зашифрованных сообщениях меток времени позволяет обеспечить защиту от повторного использования удостоверений.

Противник, перехвативший и сохранивший аутентификатор клиента, не сможет использовать его позже при условии корректной синхронизации времени. Следует, однако, иметь в виду, что большинство сетевых протоколов синхронизации времени небезопасно.

Протокол Kerberos не может защитить от атак «отказ в обслуживании» и кражи секретных ключей на стороне клиента. Полученные клиентом билеты, а также секретные ключи должны защищаться от несанкционированного доступа.

Поскольку в большинстве реализаций долговременные ключи пользователей генерируются на основании их паролей (обычно используется хэш-значение пароля), слабые пользовательские пароли позволяют реализовать атаку на основе подбора пароля. Windows Server 2012 предусматривает защиту от автономных атак подбора паролей за счет использования безопасного туннелирования между клиентом Kerberos и KDC.

Другим подходом является усиление Kerberos за счет использования цифровых сертификатов (X.509) для первоначальной аутентификации клиента на ранних этапах протокола (шаги 1–3). Такая возможность реализуется в операционных системах Windows Server в виде расширения PKINIT (Public Key Initialization). Расширение PKINIT позволяет проводить аутентификацию с помощью смарт-карт, в памяти которых хранится пара ключей (открытый и личный) клиента. Расширение PKINIT определяет следующий порядок применения цифровых сертификатов при обмене по подпротоколу AS Exchange:

- открытый ключ ОК(A) служит для шифрования сеансового ключа клиента A службой KDC,
- личный ключ ЛК(A) – для расшифрования сеансового ключа клиентом.

Тогда этап предварительной (первоначальной аутентификации) клиента в протоколе Kerberos включает следующие шаги.

1. Клиент A отсылает серверу аутентификации AS запрос, содержащий, дополнительно к стандартному, цифровой сертификат CERT клиента (с его открытым ключом ОК(A)). Метка времени в запросе подписана личным ключом клиента ЛК(A).

   $$\text{A: } \{\text{A, SS, CERT, } P_{\text{ЛК(A)}}(T_{\text{A}})\} \rightarrow \text{AS,}$$

   где $P_{\text{ЛК(A)}}$ – цифровая подпись клиента A с использованием асимметричной криптосистемы.
2. Сервер аутентификации AS проверяет действительность присланного сертификата, затем расшифровывает метку времени полученным открытым ключом клиента и проверяет ее корректность. Если проверка пройдена, клиенту направляется TGT, формируемый точно таким же образом, как при стандартном режиме аутентификации Kerberos, и клиентская информация, зашифрованная открытым ключом клиента.

AS: $\{P_{\text{ОК(А)}}(\text{ITGS}, L, K_1, T_{\text{AS}}), \text{TGT}\} \rightarrow \text{A}$,

где $P_{\text{ОК(А)}}$ – асимметричное шифрование на открытом ключе клиента А.

3. Получив сообщение, клиент расшифровывает свою часть для получения сеансового ключа K_1 имеющимся в его распоряжении личным ключом ЛК(А).

Последующие действия сторон полностью совпадают с выполняемыми в рамках стандартного протокола Kerberos. Смарт-карта, закрытый ключ и сертификат открытого ключа не используются до следующей регистрации пользователя в системе.

Методика PKINIT позволяет реализовать *двухфакторную* аутентификацию пользователя на этапе предварительной аутентификации протокола Kerberos: пользователь должен иметь смарт-карту (с хранящимися в ее памяти ключами) и знать PIN-код смарт-карты (чтобы иметь возможность использовать закрытый ключ для формирования цифровой подписи). Закрытый ключ и сертификат обычно хранятся в разных областях памяти смарт-карты.

Существуют отечественные разработки, позволяющие использовать на этапе предварительной аутентификации протокола Kerberos с PKINIT российские криптоалгоритмы (например, КриптоПро Winlogon, входящий в состав КриптоПро CSP).

Протокол SET (Secure Electronic Transaction) – протокол, специально разработанный для проведения защищенных электронных транзакций по платежным картам в недоверенной среде (например, в сети Интернет) [2]. SET защищает от подделки платежных карт, используемых для онлайн-платежей. Протокол обеспечивает конфиденциальность и целостность данных владельца карты, одновременно предоставляя средства для аутентификации карты. SET является протоколом прикладного уровня и не зависит от используемых транспортных протоколов.

SET является альтернативой использования протокола SSL/TLS при выполнении электронных платежей и рекомендован международными платежными системами Visa International и MasterCard в качестве стандарта в области электронной коммерции. По сравнению с протоколом SSL/TLS, SET имеет более узкую специализацию и не является универсальным. Функционирование протокола SET требует наличия специального программного обеспечения как на стороне сервера, так и на стороне клиента, что приводит к дополнительным издержкам. Кроме того, транзакции SET требуют больше ресурсов и работают медленнее транзакций с использованием SSL/TLS. Данные недостатки могут оказаться критичными для продавца, обрабатывающего большое число транзакций. Однако, по мнению платежных систем, это компенсируется более высоким уровнем безопасности электронных транзакций SET.

Спецификация SET поддерживает все возможности, предоставляемые современными платежными (кредитными) картами: регистрацию держателя кары, регистрацию продавца, запрос покупки, авторизацию платежа, перевод денежных средств, кредитные операции, возврат денежных средств, отмену кредита, дебитные операции.

SET позволяет потребителям и продавцам подтвердить подлинность всех участников сделки (рис. 3.3), происходящей в Интернете, средствами асимметричной и симметричной криптографии, применяя, в том числе, цифровые сертификаты. Номера на рис. 3.3 обозначают следующие операции: 1 – распределение сертификатов, 2 – формирование заказов, 3 – взаимная аутентификация, 4 – проверка счета клиента; 5 – оплата.

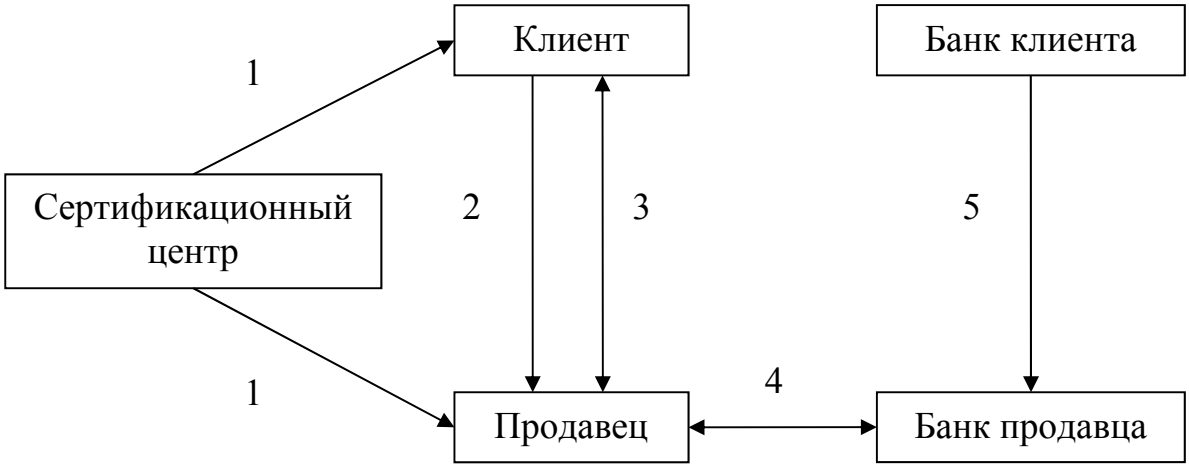


Рис. 3.3. Упрощенная схема транзакции SET

Протокол SET предоставляет сервис аутентификации для участников посредством использования сертификатов X.509. Сертификаты должны обслуживаться через определенную иерархию удостоверяющих центров. Во главе иерархической структуры находится корневой удостоверяющий центр SET Secure Electronic Transaction (LLC или SETCo).

Протокол SET защищает только финансовую информацию, непосредственно сопряженную с платежной транзакцией. Защиту информации, содержащейся в заказе, SET не регламентирует.

Интересной особенностью протокола SET является использование концепции *двойных подписей*, дающей возможность связывать два фрагмента данных и посылать их двум сущностям.

Двойная подпись формируется следующим образом:

1. Для каждого из двух подписываемых фрагментов данных формируется хэш-значение.
2. Полученные хэш-значения сцепляются и снова обрабатываются хэш-функцией.

3. Окончательное хэш-значение шифруется личным ключом подписывающего, формируя цифровую подпись.

Для шифрования SET использует как симметричные, так и асимметричные криптографические алгоритмы: сообщения шифруются на случайных ключах симметричными алгоритмами, после чего дополняются симметричными ключами и зашифровываются с помощью асимметричной схемы. Для обеспечения целостности по умолчанию используется HMAC-SHA-1, для цифровой подписи – RSA-SHA-1, симметричное шифрование по умолчанию осуществляется DES-CBC. Существенным достоинством SET является отсутствие ограничений на используемые криптоалгоритмы, что позволяет реализовать национальные стандарты шифрования.

Система SET не получила широкой популярности, и в настоящее время в качестве ее замены Visa International и MasterCard предлагают XML-протокол с поддержкой двухфакторной аутентификации пользователей. Этот протокол носит название 3-D Secure в системах Visa International и MasterCard SecureCode (MCC) в системах MasterCard.

Протокол SSH (Secure Shell, защищенная оболочка) – протокол прикладного уровня, обеспечивающий защищенную аутентификацию, соединение и безопасную передачу данных между узлами сети. Протокол реализует VPN-туннелирование для передачи данных в недоверенной среде (например, в сети Интернет), а также предоставляет возможность сжатия передаваемых данных.

Протокол широко используется для удаленного администрирования операционных систем и защищенной передачи файлов. Бесплатная версия протокола с открытым исходным кодом OpenSSH поддерживается большинством unix-платформ, предоставляя SSH-клиент и SSH-сервер в качестве стандартных утилит. В 2006 г. SHH принят в качестве интернет-стандарта.

Протокол предполагает сквозное шифрование всего трафика, обязательную аутентификацию сервера, возможность аутентификации клиента различными способами (включая использование цифровых сертификатов, аутентификацию по паролю и методы аутентификации, поддерживаемые конкретной операционной системой), обеспечение целостности и возможность сжатия передаваемых данных методом Лемпеля–Зива. Аутентификация с использованием открытых ключей является предпочтительной.

Для шифрования используется симметричный алгоритм, выбираемый в процессе переговоров сторон сеанса связи (3DES – обязательный для реализации, AES – рекомендованный, Blowfish, Twofish, CAST, Serpent в режиме CBC или потоковый шифр ARCFOUR – RC4 с 128-битным ключом). Для создания общего секретного (сеансового) ключа используется алгоритм Диффи–Хеллмана (DH) или передача в зашифрованном ви-

де (RSA с SHA1 или SHA-256). Целостность передаваемой информации обеспечивается HMAC-SHA1 (обязательный) или HMAC-MD5. Цифровые подписи используют алгоритмы RSA (рекомендованный) или DSA (обязательный) с SHA-1.

Протокол S/MIME (Secure/Multipurpose Internet Mail Extensions) – стандарт обеспечения конфиденциальности и целостности почтовых сообщений. S/MIME является протоколом прикладного уровня и предназначен для использования совместно с системами электронной почты e-mail (но не web-mail). Протокол S/MIME поддерживается, в частности, почтовыми программами Microsoft.

Хотя S/MIME наиболее известен как протокол защиты электронной почты, он может использоваться с любым транспортным механизмом, осуществляющим поддержку S/MIME, например с HTTP. S/MIME может применяться в автоматических агентах передачи сообщений, использующих криптографические сервисы. В спецификации S/MIME указывается, как использовать сервисы для шифрования факсимильных сообщений.

Конфиденциальность обеспечивается за счет симметричного шифрования 3DES (обязательный), распределение ключей производится по протоколу Диффи–Хеллмана или с использованием RSA-шифрования на открытом ключе получателя, целостность сообщений и аутентификация их источника обеспечивается с помощью технологии ЭЦП. S/MIME поддерживает цифровые сертификаты X.509 на основе RSA и алгоритмов хэширования SHA-1 (обязательный) и MD5. Должны распознаваться и цифровые подписи DSA с SHA-1. Допускается только подписание или только шифрование сообщений, а также совместное использование цифровых подписей и шифрования.

При совместном использовании шифрования и ЭЦП порядок операций определяется реализацией протокола и/или выбором пользователя. Если первым выполняется шифрование, цифровая подпись может быть проверена без вскрытия защищенной оболочки («конверта») сообщения. Такой порядок предпочтителен в системах, использующих автоматическую проверку цифровых подписей. В этом случае получатель сможет удостовериться, что блоки шифртекста не были изменены при передаче, однако он не может установить явную связь между открытым текстом присланного сообщения и отправителем. В случае использования обратного порядка операций (сначала подписание, потом шифрование) получатель сможет удостовериться в подлинности открытого текста сообщения, но не получит гарантий целостности неподписанных частей шифртекста.

Возможно совместное использование с S/MIME российских криптоалгоритмов.

3.2. Криптографическая защита систем электронного документооборота и финансовых систем

Работа современных предприятий немыслима без создания эффективной системы электронного документооборота (СЭД), позволяющей оптимизировать формирование, обработку, передачу и хранение корпоративных документов. Перед СЭД может также ставиться задача *обеспечения юридической значимости электронных документов*. Правовую основу электронного документооборота составляют нормы Гражданского кодекса РФ (часть 4), Федерального закона № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» и Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи». Согласно последнему, юридическая значимость электронного документа обеспечивается с помощью электронной подписи. Порядок использования ЭЦП в корпоративных информационных системах может устанавливаться предприятием или соглашением между участниками электронного взаимодействия.

ФЗ «Об электронной подписи» вводит понятия *простой* и *усиленной* электронной подписи, последняя может быть *усиленной неквалифицированной* и *усиленной квалифицированной* электронной подписью.

Усиленная ЭЦП должна быть получена в результате криптографического преобразования информации с использованием ключа электронной подписи, обеспечивает целостность электронного документа и позволяет определить лицо, его подписавшее. Усиленная квалифицированная электронная подпись (квалифицированная подпись) дополнительно предполагает использование квалифицированных сертификатов, а также средств генерации и проверки подписи, отвечающих специальным требованиям. На практике это означает необходимость поддержки отечественных криптоалгоритмов, сертификацию ФСБ РФ используемого программного обеспечения с криптографическими функциями и выдачу сертификата удостоверяющим центром, использующим сертифицированные ФСБ РФ СКЗИ. С криптографической точки зрения предполагается использование асимметричных криптосистем, базирующееся на инфраструктуре открытых ключей PKI.

Использование усиленной квалифицированной подписи приравнивает подписанный электронный документ к документу на бумажном носителе, заверенному собственноручно. Электронные документы, заверенные другими типами подписей, могут иметь юридическую силу по соглашению сторон (участниками электронного взаимодействия должны быть предварительно приняты соответствующие нормативные правовые акты и/или соглашения). В государственных информационных системах используется только усиленная квалифицированная ЭЦП.

Другой задачей СЭД может быть *обеспечение конфиденциального документооборота*, что предусматривает, в том числе, шифрование электронных документов при их хранении и передаче. Шифрование документов, как правило, обеспечивается симметричными криптосистемами.

Таким образом, под системой защищенного документооборота (защищенной СЭД) обычно понимается система обеспечения юридически значимого электронного документооборота, обеспечивающего конфиденциальность, целостность и имитозащиту обрабатываемых электронных документов. Под имитозащитой в этом случае понимается невозможность отправки ложного электронного документа от имени легального пользователя системы.

Защищенный юридически значимый электронный документооборот используется для:

- организации коллективной работы с документами в территориально-распределенных корпоративных информационных системах;
- обеспечения конфиденциальности и целостности документов;
- подтверждения авторства (аутентичности) документов и невозможности отказа от авторства;
- обеспечения доверия пользователей к содержанию электронных документов;
- регламентации доступа пользователей к документам.

«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные руководством 8 Центра ФСБ РФ 21.02.2008 № 149/54-144, требуют использования сертифицированных ФСБ РФ СКЗИ для защиты персональных данных. Использование сертифицированных СКЗИ потребуется и для защиты государственных информационных систем, в том числе для построения защищенных СЭД. Согласно Приказу ФСБ РФ от 27 декабря 2011 г. № 796, содержащему «Требования к средствам электронной подписи» и «Требования к средствам удостоверяющего центра», СКЗИ, имеющие в своем составе функции по созданию и проверке электронных подписей, должны:

при создании электронной подписи:

- показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
- создавать ЭЦП только после подтверждения операции по созданию подписи лицом, подписывающим электронный документ;
- однозначно показывать, что ЭЦП создана;

при проверке электронной подписи:

- показывать содержание подписанного электронного документа;
- показывать информацию о внесении изменений в подписанный электронный документ;
- указывать на лицо, с использованием ключа которого подписаны электронные документы.

В современных условиях электронный документооборот, как правило, выходит за внутрикорпоративные рамки (например, предприятия сдают электронную бухгалтерскую отчетность в налоговые органы), поэтому предпочтительным является использование квалифицированной электронной подписи. Удостоверяющий центр, выдающий квалифицированные сертификаты, должен иметь лицензии ФСБ на осуществление деятельности, связанной с криптографическими средствами, пройти аккредитацию в Министерстве связи и массовых коммуникаций и подключиться к сети доверенных удостоверяющих центров (ФНС и, при необходимости, других государственных служб). Удостоверяющий центр часто также имеет лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации. Возможно создание удостоверяющего центра собственными силами крупной компании, однако, как правило, прибегают к услугам стороннего доверенного центра сертификации.

Таким образом, невозможно избежать необходимости передачи электронных документов по открытым сетям (через Интернет), что может также обусловливаться территориальной распределенной структурой самой компании и/или необходимостью организации работы мобильных пользователей. Все это требует организации защищенных VPN-подключений, которые могут быть реализованы средствами стандартных защищенных сетевых протоколов (SSL и TLS для передачи в Интернет и IPSec – в рамках локальной сети), в том числе, при необходимости, на базе сертифицированных криптопровайдеров (CSP), поддерживающих российские криптографические стандарты.

Возможная структура защищенной СЭД представлена на рис. 3.4. Работа во внутренней сети организована по принципу «тонкого клиента», т. е. большая часть операций СЭД выполняется непосредственно на сервере.

Система защиты информации включает подсистемы:

- аутентификации пользователей;
- управления доступом;
- регистрации и учета событий;
- контроля целостности;
- управления пользователями;
- криптографической защиты.

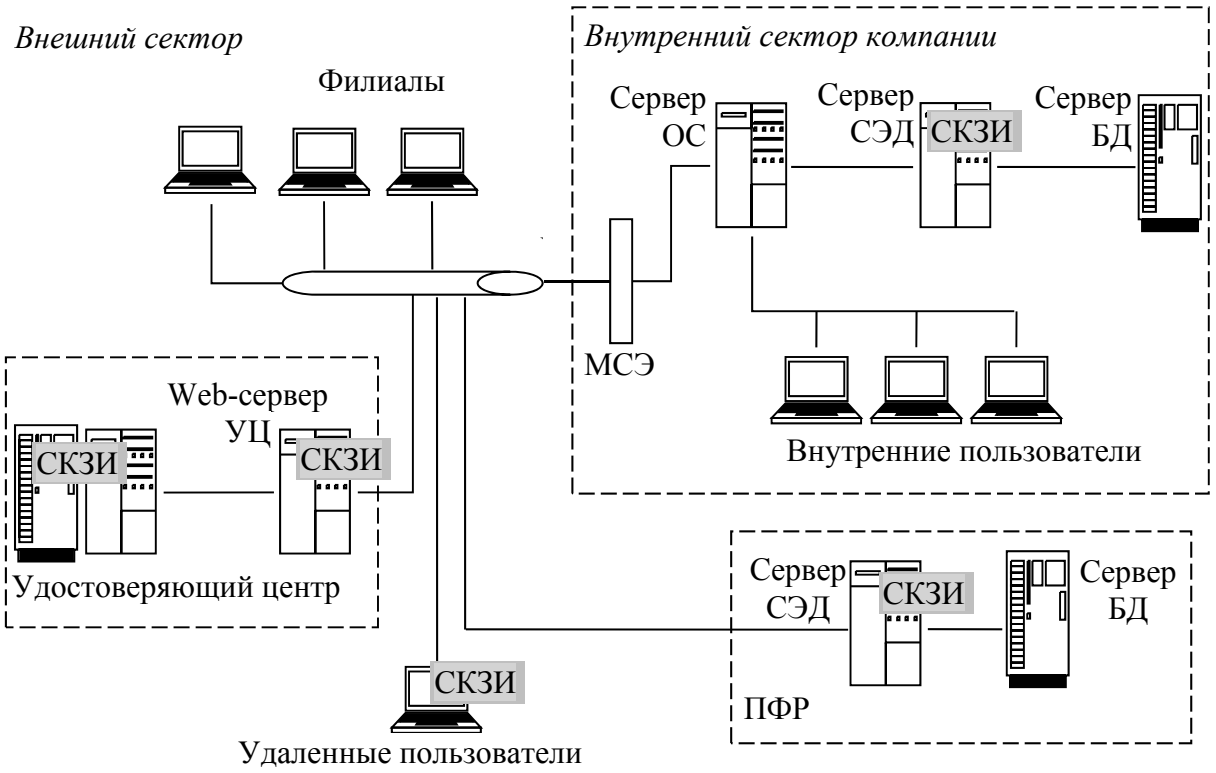


Рис. 3.4. Пример защищенной СЭД

Криптографический модуль системы защиты СЭД обеспечивает работу с электронной подписью и обращение к доверенному центру сертификации, а также прозрачное шифрование информации с целью ее безопасного хранения и передачи. Он также может являться частью подсистемы аутентификации пользователей, поддерживая использование отчуждаемых ключевых носителей (смарт-карт, USB-токенов). Этот вариант предпочтительнее, так как позволяет хранить секретные ключи, используемые как для аутентификации, так и для подписывания документов, на внешних носителях.

Информационные системы, используемые в банковском и кредитно-финансовом секторе, по сути, представляют собой защищенные СЭД, и отличаются, как правило, большой степенью модульности и сложной, территориально-распределенной структурой. Согласно стандарту Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», в банковских информационных системах необходимо использовать СКЗИ, которые сертифицированы уполномоченным государственным органом либо имеют разрешение ФСБ России; СКЗИ, применяемые для защиты персональных данных, должны иметь класс не ниже КС2. Необходимость использования СКЗИ определяется организацией БС РФ самостоятельно, если иное не предусмотрено законодательством РФ.

В системах электронных платежей с использованием платежных карт необходимо использовать средства защиты, соответствующие требованиям стандарта безопасности данных индустрии платежных карт (PCI DSS v.3.0, Payment Card Industry Data Security Standard). PCI DSS предусматривает использование стойких криптографических алгоритмов для защиты данных держателей карт при их хранении и передаче, а также внедрение процедур управления ключами.

Запрещается хранение после авторизации: критических аутентификационных данных (кроме эмитентов карт), полного содержимого магнитной полосы карты, CVC- и PIN-кодов, даже в зашифрованном виде. Для хранения номеров платежных карт PAN используются однонаправленные хэш-функции или стойкое шифрование. При передаче данных через общедоступные сети применяются надежные криптографические алгоритмы и протоколы защиты (например, SSL/TLS, IPSec, SSH и т. д.) с использованием только доверенных ключей и сертификатов. Стойкое шифрование должно быть обеспечено и при использовании беспроводных сетей.

Библиографический список

1. Рекомендация X.800. Сети передачи данных: взаимосвязь открытых систем (ВОС); безопасность, структура и приложения. Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ. – Женева, 1991 [Электронный ресурс]. – URL: http://www.itu.int/ rec/T-REC-X.800-199103-I/e (дата обращения: 05.10.2015).
2. *Бернет С.*, *Пэйн С.* Криптография. Официальное руководство RSA Security. – М.: ООО «Бином-Пресс», 2009.
3. *Мамаев М.*, *Петренко С.* Технологии защиты информации в Интернете: Специальный справочник. – СПб.: Питер, 2001. – 848 с.
4. *Шнайер Б.* Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2012. – 816 с.

3.3. Программно-аппаратные средства криптографической защиты информации

Практическая криптография распространяется все шире вслед за развитием электронного документооборота, широкодоступных сетевых служб, обмена информацией через сети общего пользования. Средствами криптографической защиты информации (СКЗИ) решается множество задач, непосредственно связанных с обеспечением информационной без-

опасности любой системы, базы данных или сети передачи информации. Кроме того, существует ряд направлений, в которых применение СКЗИ практически не имеет альтернативы:

- защищенная электронная почта (электронный документооборот);
- обеспечение безопасности электронных транзакций (электронные платежи);
- виртуальные частные сети (VPN).

В качестве СКЗИ наиболее широко используют три вида шифраторов:

- программные,
- аппаратные,
- программно-аппаратные.

Их основное различие заключается не только в способе реализации шифрования и степени надежности защиты данных, но и в цене, что часто становится для пользователей определяющим фактором.

Программные СКЗИ отличают низкая стоимость, большая гибкость в реализации, возможность неограниченного тиражирования и высокая мобильность. Однако в общем случае работу программного средства нарушить легче, чем его аппаратного аналога, что требует дополнительного контроля ошибок функционирования. Другим важным требованием является необходимость обеспечения конфиденциальности ключевой информации, что достигается за счет использования иерархии ключей и отчуждения мастер-ключа (ключа шифрования ключей) от информационной системы (например, за счет хранения на внешнем носителе – токене, смарт-карте).

Можно выделить следующие основные функции программных СКЗИ [1]:

- идентификация и аутентификация пользователей;
- обеспечение криптографической защиты операционных систем и приложений;
- генерация псевдослучайных последовательностей;
- шифрование данных на носителях, в том числе «прозрачное» шифрование;
- формирование и проверка ключевой информации, электронных подписей, защита от копирования программного кода;
- безопасное распределение ключевой информации при инициализации СКЗИ, в том числе аппаратных.

Доминирующее положение операционной системы Windows на рынке обусловливает внимание к программным интерфейсам библиотек криптографических функций (криптографическим интерфейсам) этой операционной системы – *Crypto API*, *CNG API*.

API (Application Programming Interfaces) – интерфейс программирования приложений, API определяет функциональность, которую предоставляет программа (модуль, библиотека), при этом API позволяет абстрагироваться от того, как именно эта функциональность реализована.

Crypto API – это интерфейс программирования приложений, который предоставляет разработчикам Windows-приложений средства вызова криптографических функций. В основе шифрования Windows Vista, Windows Server 2008 и более поздних версий операционной системы лежит новый криптографический интерфейс, называемый CNG API (Cryptography Next Generation). Основными отличиями CNG API являются: отделение хранилищ ключей от операций алгоритма, изоляция процессов для операций с долговременными ключами, подключаемые генераторы случайных чисел, криптографический API режима ядра и отсутствие ограничений на экспорт.

Криптографические интерфейсы Windows, с одной стороны, позволяют включать по мере разработки новые функции, а с другой – не требуют после этого изменения и обновления всех ранее созданных приложений. Для реализации такого интерфейса выбрана структура пакета, в которой обращение к функциям API представляет собой уровень связи с приложениями, а за ним располагается другой уровень, открытый для обновления и включения новых функций в виде встраиваемых компонентов, в том числе и от независимых разработчиков. Эта структура иллюстрируется рис. 3.5.

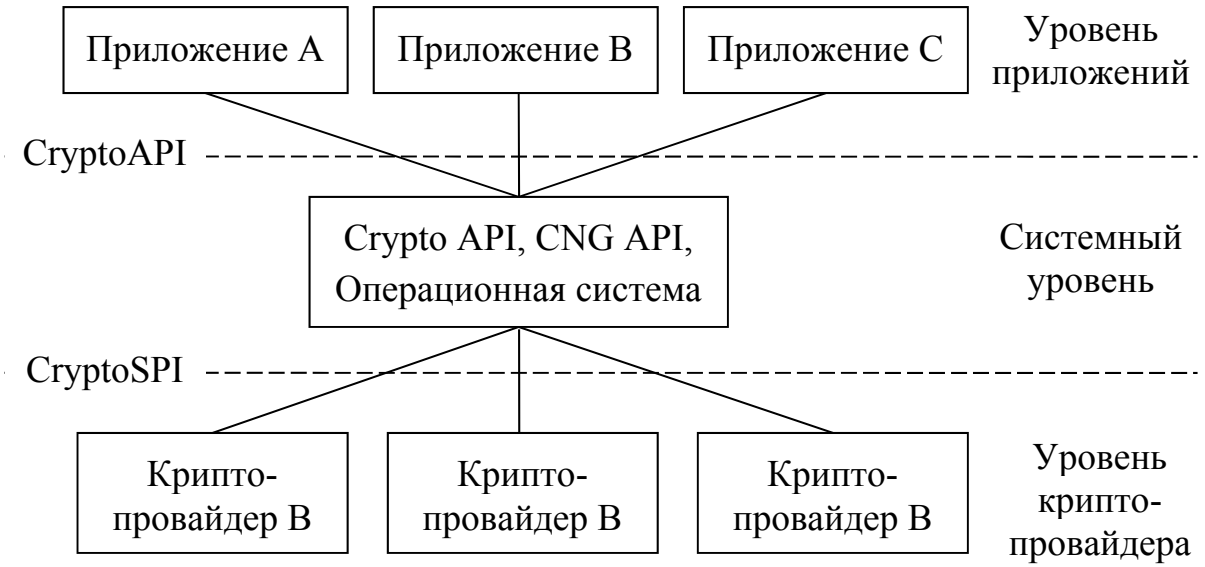


Рис. 3.5. CryptoAPI обеспечивает взаимодействие между приложением и провайдерами службы шифрования

Встраиваемый компонент, позволяющий осуществлять отдельные криптографические операции (шифрование, электронная подпись и т. д.) в операционной системе и реализующий криптографические алгоритмы, в терминологии Microsoft называется провайдером службы шифрования – CSP (Cryptographic Service Provider).

По своей сути криптопровайдеры CSP являются независимыми модулями (независимыми динамическими библиотеками DLL или вообще отдельными сервисами), предоставляющими криптографические функции пользовательским приложениям. Они подписаны цифровой подписью, так что система может проверять их подлинность. В составе операционной системы Windows пользователь получает несколько таких CSP, которые реализуют наиболее часто используемые методы шифрования. Если разрабатываемое приложение нуждается в стороннем компоненте CSP, это никак не отражается на программировании самого приложения. Оно строится точно так же, как если бы в нем использовался один из «родных» компонентов Windows.

В такой структуре на криптографический интерфейс практически не возлагаются иные функции, кроме передачи сообщений между приложением и выбранными для приложения CSP. Поэтому при необходимости можно достаточно быстро настроить приложение на другой алгоритм шифрования, указав при вызове функций CryptoAPI новый компонент CSP.

Таким образом, еще одним достоинством криптографических интерфейсов Windows является возможность замены в уже разработанном приложении одной библиотеки криптографических функций на другую, более современную, созданную заслуживающей большего доверия организацией или реализующую более стойкие криптографические алгоритмы и протоколы. Причем эта замена может быть произведена без какой-либо переделки самой прикладной программы.

CSP отличаются друг от друга своими типами, которые определяются набором параметров, включающим:

- алгоритм обмена сессионным (симметричным) ключом,
- алгоритм вычисления цифровой подписи,
- формат цифровой подписи,
- схему генерирования сессионного ключа по хэшу,
- длину ключа.

Разработан ряд криптопровайдеров, поддерживающих отечественные стандарты криптографических алгоритмов ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012, ГОСТ 28147–89 (КриптоПро CSP, ViPNet CSP, Shipka Base Cryptographic Provider GOST, Валидата CSP и др.) и имеющих сертификат ФСБ РФ. Использование этих криптопровайдеров позволяет соблюсти,

если это необходимо, требование об обязательном использовании сертифицированных СКЗИ.

Архитектура Crypto API может быть разделена на три основные части:

- базовые функции,
- функции для работы с сертификатами,
- функции для работы с сообщениями.

В первую группу входят функции для выбора и подключения к криптопровайдеру, генерации и хранения ключей, обмена ключами, выбора режима алгоритмов блочного шифрования (CBC или ECB), а также криптографическая функция генерации случайных данных. К базовым относятся также функции для хэширования и получения цифровой подписи данных, шифрования и расшифрования.

Во вторую группу входят функции для использования сертификатов, основной задачей которых является предоставление доступа к открытому ключу. Crypto API поддерживает сертификаты спецификации X.509, в которые входит информация о версии сертификата, его серийном номере, периоде действия, алгоритмах шифрования публичного ключа.

Под сообщениями в Crypto API понимаются данные в стандартизованном формате PKCS #7, разработанном RSA Laboratories. Функции для работы с ними делятся на две части: высокоуровневые функции (упрощенные) и низкоуровневые.

Зачастую применение непосредственно функций Crypto API достаточно проблематично. Например, в web-клиентах, где вызовы процедур напрямую невозможны. Для подобных целей, а также для упрощения работы с Crypto API был создан тип объектов CAPICOM (Crypto API COM-object). В своей реализации данный объект почти полностью охватывает все – от шифрования до работы с сертификатами.

Платформа .NET Framework позволяет работать с функциями Crypto API (CNG API) в объектно-ориентированной среде посредством набора классов в пространстве имен System.Security.Cryptography. Пространство System.Security.Cryptography содержит основные симметричные шифры (DES, 3DES, AES, Rijndael, RC2) и асимметричные криптосистемы (RSA, DSA, ECDSA, система Диффи–Хеллмана на эллиптических кривых), несколько хэш-функций (MD5, SHA-1, SHA-2, RIPEMD160), кодов аутентификации (HMAC-SHA-1, HMAC-SHA-2, HMAC-RIPEMD, MAC-3DES) и криптографически сильный генератор псевдослучайных чисел. Эта криптографическая основа может быть расширена за счет подключения CSP сторонних производителей. Расширения криптографической объектной модели .NET Framework могут быть двух типов: добавление новой реализации криптоалгоритма, уже определенного в .NET Framework, или добавление нового криптоалгоритма.

Пространство имен System.Security.Cryptography содержит следующие основные классы:

- SymmetricAlgorithm – симметричные шифры;
- AsymmetricAlgorithm – криптосистемы с открытым ключом;
- CryptoStream – поддерживает модель программирования на основе потоков (streams), представляющих данные из разных хранилищ (текстовых файлов, XML-документов, памяти, сети), при криптографических преобразованиях;
- CspParameters – передает параметры криптопровайдеру CSP, который выполняет криптографические преобразования;
- HashAlgorithm – функции хэширования и коды аутентификации;
- RandomNumberGenerator – генератор псевдослучайных последовательностей;
- классы Cryptography Next Generation (CNG) – для прямого вызова криптографических API функций. Центральным является класс CngKey – хранение и использование CNG-ключей, также реализованы поддерживающие CNG классы: CngProvider – провайдер хранилища ключей, CngAlgorithm и CngAlgorithmGroup – реализованные средствами CNG алгоритмы шифрования или группы алгоритмов (CngKey получает объекты CngAlgorithm через параметр algorithm и возвращает объекты CngAlgorithmGroup), CngUIPolicy – политика пользовательского интерфейса, относящегося к операциям с ключами.

Перечисленные классы являются абстрактными базовыми классами, которые инкапсулируют другие классы, специфичные для конкретных криптоалгоритмов. Производные классы реализуют конкретные публичные свойства и виртуальные методы абстрактного базового класса в зависимости от используемого криптоалгоритма.

Пространство имен System.Security.Cryptography.XML реализует цифровую подпись XML-объектов, а System.Security.Cryptography.X509 Certificaties обеспечивает поддержку операций с цифровыми сертификатами.

Аппаратные шифраторы представляют собой, как правило, плату, подключаемую к системной плате компьютера посредством разъемов ISA или PCI. Реже устройство выполняют в виде отдельного средства защиты, обладающего корпусом с дисплеем и переключателями режимов. Так как использование отдельной платы для выполнения исключительно шифрования является нецелесообразным, производители снабжают устройства дополнительными функциями: генерация случайных чисел, контроль целостности программных файлов, контроль доступа к информации и т. д. Плата с перечисленными выше функциями представляет собой аппаратное средство криптографической защиты информации (СКЗИ).

Шифратор, выполняющий контроль входа на ПК и проверяющий целостность операционной системы, называют также «электронным замком». Такое устройство должно иметь соответствующее программное обеспечение, а для корректной работы необходима его настройка администратором безопасности. При включении компьютера устройство криптографической защиты данных будет запрашивать ключи и не позволит продолжить загрузку, пока они не будут корректно введены. В случае передачи управления компьютеру встроенные в шифратор функции через некоторое время заблокируют работу пользователя. Это в полной мере защитит информацию от попыток несанкционированного доступа к ней.

Аппаратный шифратор – надежное, но более дорогостоящее по сравнению с программными реализациями СКЗИ. Приобретение аппаратного шифратора целесообразно, прежде всего, для компаний, обрабатывающих большие объемы конфиденциальной информации, например в налоговой или банковской сфере. Заказчик может выбрать состав и функциональность устройства исходя из специфики его компании. Дополнительные функции позволят защитить информацию не только от утечек по каналу связи, но и от несанкционированного доступа к компьютерной системе.

На российском рынке СКЗИ представлены устройства компаний ОКБ САПР (Аккорд), «Анкад» (Криптон) и «Код безопасности», представляющие собой программно-аппаратные комплексы защиты информации, в состав которых входят, в том числе, аппаратные шифраторы, а также аппаратно-программные модули доверенной загрузки, системы разграничения доступа, мониторинга и другие компоненты. Указанные СКЗИ поддерживают российские криптографические стандарты и имеют сертификаты ФСБ РФ.

СКЗИ, использующиеся в системах защиты следующих сведений, не составляющих государственную тайну: персональные данные, служебная тайна (служебная информация государственных и муниципальных органов власти), подлежат обязательной сертификации ФСБ РФ, для банковской информации такая сертификация носит рекомендательный характер (в соответствии со СТО БР ИББС).

Можно выделить минимальный набор функций, которыми должен обладать типовой шифратор [2]:

- реализация отечественных криптоалгоритмов ГОСТ 28147–89 (ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012);
- программный интерфейс;
- возможность аутентификации пользователя;
- наличие датчика случайных чисел;
- реализация защищенного сетевого протокола;
- поддержка ввода ключей с ключевых носителей.

При проектировании аппаратного шифратора производитель может добавлять дополнительные микросхемы для обеспечения надежности процессов шифрования. Однако все аппаратные СКЗИ имеют одинаковый набор базовых функциональных модулей. Основными модулями аппаратного СКЗИ являются:

1) Блок управления. Обычно реализуется на базе микроконтроллера. Блок управления предназначен для управления работой СКЗИ: переключения режимов работы, определения состояния СКЗИ при включении и управлении в процессе работы, осуществления взаимодействия со средствами ввода ключевой информации.

2) Шифропроцессор. Представляет собой специализированную микросхему или микросхему программируемой логики (PLD – Programmable Logic Device). Шифропроцессор выполняет криптографические преобразования данных на ключах, которые хранятся в энергонезависимых банках памяти. Блок шифропроцессора состоит, как правило, из основного и дублирующего шифраторов, предназначенных для дублированного выполнения процедур шифрования. Результаты основного и дублирующего шифрования сравниваются с целью контроля исправности функционирования.

3) Блок датчика случайных чисел (ДСЧ). Предназначен для формирования запаса псевдослучайных последовательностей, используемых при генерации ключей шифрования, вычисления имитовставки и электронной подписи. Датчик случайных чисел может быть реализован как программно на базе шифропроцессора, так и физически в виде отдельной микросхемы. Принцип работы физического ДСЧ основан на выработке случайного сигнала, который преобразуется в двоичную последовательность.

4) Блок подключения внешних устройств. Управляет процессом взаимодействия СКЗИ с внешними устройствами. Обеспечивает подключение к компьютеру, обмен командами и данными между шифратором и внешними устройствами. Может быть реализован на микросхеме управления СКЗИ.

5) Блок долговременного хранения ключевой информации. Представляет собой энергонезависимую память, в которой хранятся комплекты основных и резервных ключей, файлы программного обеспечения СКЗИ, журналы с результатами контроля исправности и др. Ключевая информация хранится в зашифрованном и имитозащищенном виде. Для обеспечения целостности рассчитывается контрольная сумма, проверяемая при каждом включении устройства. Считывание и запись в блок осуществляется блоком управления СКЗИ.

6) Блок ввода ключевой информации. Предназначен для ввода в устройство ключевой информации при начальной инициализации устройства. Ключевая информация вводится с ключевых носителей типа смарт-карт с одновременным контролем ввода путем проверки контрольных

сумм. Хранение ключей на смарт-картах и их ввод в устройство с помощью интерфейсов для подключения ключевых носителей позволяет обеспечить более надежную защиту.

Для повышения надежности процесса шифрования, модификации ключей и проверки правильности результатов шифрования шифропроцессор (ЦСП) логически разделяют на несколько функциональных блоков:

1) Вычислитель – набор регистров, сумматоров, блоков подстановки, связанных между собой шинами передачи данных. Выполняет криптографические действия с данными. На вход вычислитель получает открытые данные, которые зашифровывает с помощью ключа шифрования. Зашифрованная выходная последовательность данных схожа с последовательностью случайных величин.

2) Блок управления – аппаратно реализованная логика управления вычислителем. Сбои в работе блока могут привести к некачественному шифрованию, вследствие чего возможны утечки информации в канал связи. С целью повышения надежности шифратора используется программно-временное дублирование процесса шифрования. Два шифратора (основной и дублирующий) преобразовывают одинаковые входные данные со сдвигом в алгоритме на один шаг. Конечный результат поступает в микросхему сравнения для проверки. При несовпадении результатов данные зашифровываются повторно.

3) Буфер ввода-вывода. Необходим для повышения производительности устройства: в процессе шифрования первого блока данных в буфер поступает следующий блок и т. д. Алгоритм вывода информации аналогичен. Такой способ передачи данных значительно увеличивает скорость процедур шифрования и дешифрования.

Наряду с доступной функциональностью важны эксплуатационные качества аппаратного СКЗИ, которые определяются скоростью выполнения операций, уровнем надежности, а в ряде случаев – и уровнем защищенности, т. е. способностью противостоять целенаправленным воздействиям. Применение детекторов воздействий и дополнительного экранирования позволяет повысить защищенность шифратора, однако может существенно увеличить стоимость реализации, поэтому целесообразно лишь для отдельных сфер применения (например, в военной области).

Одним из важнейших критериев оценки аппаратных шифраторов является потоковая скорость обработки данных. Главным образом она зависит от реализованного в шифраторе криптоалгоритма. Потоковая скорость оценивается по формуле $V = F*k / n$, где F – тактовая частота микропроцессора, k – размер блока информации, подлежащей шифрованию, n – число тактов алгоритма, требующихся для шифрования одного блока информации [3].

Аппаратные шифраторы чаще всего реализуются на базе сигнальных процессоров (цифровых сигнальных процессоров, ЦСП), обладающих вы-

соким быстродействием. Эффективность выполнения основных функций шифратора и его надежность в наибольшей степени определяются используемым ЦСП, который является центральным критическим компонентом элементной базы шифратора. Анализ рынка показывает практическое отсутствие отечественных производителей элементной базы аппаратных шифраторов, лидерами в производстве микросхем являются компании Texas Instruments, Freescale Semiconductor и Analog Devices [4].

СКЗИ должны обеспечивать заданный уровень надежности применяемых криптографических преобразований, определяемый значением допустимой вероятности неисправностей или сбоев, которые могут привести к потенциально опасным последствиям:

- утечка открытой информации в канал связи;
- утечка ключевой и криптографически опасной информации в канал связи;
- несанкционированный доступ к ключевой и криптографически опасной информации;
- попадание конфиденциальной информации, подлежащей шифрованию, к техническому персоналу в незашифрованном виде.

Надежность является комплексным свойством, которое в зависимости от назначения СКЗИ и условий его применения может включать безотказность, долговечность, ремонтопригодность и сохраняемость или определенные сочетания этих свойств. В основе определения вероятностей сбоев, приводящих к возникновению потенциально опасных событий, лежит расчет интенсивности отказов составных элементов шифратора. СКЗИ, не предназначенные для защиты сведений, составляющих государственную тайну, должны соответствовать «Требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну», согласно положению (ПКЗ-2005), утвержденному приказом ФСБ РФ от 09.02.2005 г. № 66. Указанные требования предусматривают соответствие значений вероятностей и классов защищенности СКЗИ.

Соответствие значений вероятностей возникновения опасных событий для используемых ЦСП и значений вероятностей, регламентируемых требованиями к СКЗИ, определяет класс СКЗИ, а следовательно, возможность его применения в системах защиты конфиденциальной информации.

Библиографический список

1. *Васильева И.Н.* Криптографическая защита информации: учеб. пособие. – СПб.: СПбГИЭУ, 2011. – 248 с.
2. *Васильева И.Н.*, *Семенова С.О.* Состав и характеристики аппаратных шифраторов // Образование и наука: современное состояние и перспек-

тивы развития: сборник научных трудов по материалам Международной научно-практической конференции 31 августа 2015 г. – Тамбов, 2015. – С. 19-23.
3. *Панасенко С.П.*, *Ракитин В.В*. Аппаратные шифраторы // Мир ПК. – 2002. – № 8. – С. 77-83.
4. *Пантелейчук А.Р*. Основы выбора цифровых сигнальных процессоров // Электронные компоненты. – 2010. – № 6. – С. 13-17.

Глава 4. ЭКОНОМИЧЕСКИЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Методика оценки экономического эффекта использования ИТ-аутсорсинга с учетом риска сотрудничества с внешним провайдером услуг

В настоящее время основным критерием перехода на аутсорсинг (в том числе, и в области информационных технологий) является снижение затрат по сравнению с выполнением процесса собственными силами предприятия. Однако сотрудничество с аутсорсером может привести к росту рисков для информационной и экономической безопасности предприятия. Это означает, что при принятии решения об использовании ИТ-аутсорсинга заказчик должен учитывать не только изменение затрат, но и изменение уровня рисков по сравнению с выполнением соответствующих функций собственными силами. Таким образом, существует потребность в разработке методики оценки экономического эффекта ИТ-аутсорсинга с учетом рисков сотрудничества с внешним провайдером услуг.

Методика опирается на понятие полной стоимости информационной системы, которая включает в себя затраты на создание и эксплуатацию информационной системы и потери от ее ненадлежащего функционирования.

Использование аутсорсинга в сфере информационных технологий получило широкое распространение благодаря ряду преимуществ, которые получает заказчик (сразу следует отметить, что мы используем термин «аутсорсинг» в широком смысле слова, относя к нему все модели систематического привлечения внешнего подрядчика для выполнения необходимых заказчику задач, процессов и функций; в частности, мы относим к аутсорсингу облачные технологии) [1, 2]. К числу этих преимуществ относятся:

- возможность получить доступ к уникальным ресурсам, отсутствующим у самого заказчика (приобретение этих ресурсов заказчиком в собственность неоправданно с экономической точки зрения, поскольку у него может не быть необходимых компетенций для эксплуатации таких ресурсов или заказчик не сможет обеспечить их полноценную загрузку и по этой причине не получит экономию на масштабе, или же просто стоимость этих ресурсов намного превышает финансовые возможности заказчика). К таким ресурсам относятся специализированное программное и аппаратное обеспечение, базы данных, каналы связи и т. д. Иными словами, заказчик может, пользуясь эффектом сервисного рычага [9], значительно увеличить объем доступных ему ресурсов, не инвестируя в их формирование, а получая временный доступ к ними, тем самым, наращи-

вая свой производственный потенциал. Фактически речь нередко идет о возникновении у заказчика принципиальной возможности выполнять соответствующий процесс за счет использования внешних ресурсов;

- повышение качества выполнения процесса благодаря более высокой производительности внешних ресурсов и более высокому уровню профессиональной подготовки персонала внешнего подрядчика;

- снижение издержек выполнения процесса и управленческих издержек (благодаря высокой специализации аутсорсера, высокой производительности его активов и наличию эффекта экономии на масштабе производства, а также улучшению организационной структуры предприятия – фактически аутсорсинг может выступать в качестве инструмента реструктуризации фирмы [11]).

Целесообразность перехода к аутсорсингу (и выбор аутсорсера), таким образом, определяется путем оценки тех выгод, которые заказчик получит от использования преимуществ аутсорсинга. Соответствующее решение принимается на основе расчета простого или сложного (интегрального, учитывающего различные технико-экономические параметры процесса или функции, передаваемых на аутсорсинг) показателя ожидаемого эффекта от использования аутсорсинга (в настоящее время предложено значительное число методик для расчета таких показателей, как носящих общий характер, так и адаптированных для потребностей определенных отраслей; для расчета интегральных показателей существует широкий спектр процедур свертки).

Тем не менее, наряду с достоинствами, аутсорсингу присущи и значительные недостатки, среди которых первое место занимает зависимость от аутсорсера (из-за неспособности заказчика своими силами выполнить переданный процесс или функцию). Эта зависимость влечет за собой риск того, что аутсорсер пожелает злоупотребить ею (чтобы вынудить заказчика к более выгодным для себя условиям сотрудничества). Также возникает риск того, что аутсорсер по тем или иным причинам просто не справится с выполнением переданного ему процесса, тем самым поставив под угрозу собственную хозяйственную деятельность заказчика. Наконец, существует риск того, что аутсорсер злоупотребит переданной ему в ходе выполнения договора информацией о внутренней деятельности заказчика.

При этом важно отметить, что аутсорсинговый контракт является договором, заключенным между двумя независимыми и равноправными участниками хозяйственной деятельности, и у заказчика нет никаких официальных рычагов принуждения аутсорсера к исполнению своих контрактных обязательств иначе, как по суду. Инструменты административного иерархического принуждения, типичные для внутрифирменных отношений, при аутсорсинге (как при межфирменной сделке) отсутствуют.

Таким образом, избавляясь от затрат на выполнение соответствующего процесса, заказчик одновременно лишается контроля над его исполнением.

Это означает, что заказчику при принятии решения об использовании аутсорсинга необходимо не просто рассчитать предполагаемый экономический эффект, но также учесть возможные потери, связанные с реализацией рисков аутсорсинга. Особенно это важно в такой чувствительной области, как информационные технологии. В современных условиях ненадлежащее функционирование информационной системы может привести к таким тяжким последствиям, как нарушение непрерывности существования предприятия [3, 4], что требует применения системы риск-менеджмента при реализации аутсорсинговых проектов.

Цель данного исследования состоит в разработке алгоритма принятия решения об использовании аутсорсинга в области информационных технологий с учетом рисков. Иными словами, мы будем рассматривать проблему сотрудничества с аутсорсером с точки зрения обеспечения информационной и экономической безопасности предприятия.

Сразу следует оговориться, что в настоящее время есть ряд публикаций, в которых исследуется проблема оценки риска аутсорсинга (к числу наиболее важных, на наш взгляд, следует отнести работы И.Д. Котлярова [7, 8], Д.В. Грошкова [5]). Однако эти исследования в основном направлены на оценку рисков аутсорсинга, тогда как вопрос учета влияния этих рисков на ожидаемый экономический результат от сотрудничества с аутсорсером в них практически не затрагивается. Кроме того, эти работы не учитывают специфику информационных технологий (ИТ). Интересно отметить, что в публикациях по аутсорсингу в ИТ (весьма многочисленных) проблема учета рисков при принятии решения об использовании аутсорсинга не затрагивается либо затрагивается вскользь (авторы упоминают о необходимости учета рисков аутсорсинга, однако методики оценки этих рисков не предлагают).

Очевидно, что риски сотрудничества с аутсорсером могут быть оценены в денежном выражении, поскольку их реализация влечет за собой финансовые потери для заказчика. Отсюда, в соответствии с методикой, предложенной В.А. Тушавиным [11] и развитой И.Д. Котляровым [10], можно ввести понятие полной стоимости информационной системы предприятия F, которая включает в себя как затраты на создание и функционирование этой системы (включая обеспечение ее безопасности), так и возможные потери предприятия в случае ненадлежащего функционирования этой системы.

В таком случае полную стоимость информационной системы (ИС) предприятия при обеспечении ее создания и функционирования силами самого предприятия F_{own} можно представить в следующем виде:

$$F_{own} = C_{own} + W_{own,\text{int}} L_{own,\text{int}} + W_{own,ext} L_{own,ext} + W_{NA,own} L_{NA,own}\,, \qquad (1)$$

где C_{own} – собственные затраты предприятия на создание и обеспечение функционирования ИС;

$L_{own,\text{int}}$ – размер потерь предприятия в случае несанкционированного или недобросовестного использования ИС со стороны внутренних пользователей при самостоятельном создании и обеспечении функционирования ИС предприятием. Примером может быть ситуация, когда сотрудник трейдинговой компании может самостоятельно снять ограничение на максимально разрешенный ему объем сделок;

$W_{own,\text{int}}$ – вероятность наступления потерь от несанкционированного или недобросовестного использования ИС со стороны внутренних пользователей при самостоятельном создании и обеспечении функционирования ИС предприятием. Может быть определена экспертно или путем анализа уже имеющегося опыта эксплуатации ИС.

Очевидно, что произведение $W_{own,\text{int}} L_{own,\text{int}}$ имеет смысл математического ожидания потерь предприятия в случае несанкционированного или недобросовестного поведения внутренних пользователей. Столь же очевидно, что число вариантов такого поведения очень велико и каждый вариант будет характеризоваться определенным размером потерь и определенной вероятностью наступления, поэтому, строго говоря, нам бы следовало использовать запись $\sum_{i=1}^{n} W^i_{own,\text{int}} L^i_{own,\text{int}}$. Однако для краткости и во избежание громоздких формул мы будем использовать обозначение $W_{own,\text{int}} L_{own,\text{int}}$, имея в виду, что подразумевается запись $\sum_{i=1}^{n} W^i_{own,\text{int}} L^i_{own,\text{int}}$;

$L_{own,ext}$ – размер потерь предприятия в случае недобросовестного или несанкционированного использования ИС предприятия со стороны внешних пользователей (при создании и обеспечении функционирования ИС силами предприятия). В качестве примеров можно привести DDOS-атаку на сервер компании, взлом ее платежной системы или кражу клиентской информации;

$W_{own,ext}$ – вероятность наступления потерь несанкционированного или недобросовестного поведения со стороны внешних пользователей;

$L_{NA,own}$ – размерь потерь предприятия в случае ненадлежащего функционирования ИС (технические сбои). Пример: «зависание» самостоятельно созданного предприятием программного обеспечения;

$W_{NA,own}$ – вероятность ненадлежащего функционирования ИС в случае ее создания и поддержки силами самого предприятия.

Аналогично, в том случае, если создание и функционирование ИС обеспечивается силами аутсорсера, то полная стоимость ИС F_{out} будет равна:

$$F_{out} = C_{out} + W_{out,\text{int}} L_{own,\text{int}} + W_{out,ext} L_{own,ext} + W_{out} L_{out} + W_{NA,out} L_{NA,out}, \quad (2)$$

где C_{out} – плата аутсорсеру за создание и поддержку ИС;

$L_{out,\text{int}}$ – размер потерь заказчика от недобросовестного или несанкционированного поведения внутренних пользователей в случае создания и поддержки ИС силами аутсорсера;

$W_{out,\text{int}}$ – вероятность недобросовестного или несанкционированного поведения внутренних пользователей;

$L_{out,ext}$ – размер потерь заказчика от недобросовестного или несанкционированного поведения внешних пользователей;

$W_{out,\text{ext}}$ – вероятность наступления потерь от недобросовестного или несанкционированного поведения внешних пользователей. Отметим, что, по нашему мнению, к числу внешних пользователей относится провайдер, обеспечивающий доступ заказчика к информационным ресурсам аутсорсера (как известно, при использовании облачных технологий необходимые заказчику информационные ресурсы используются в удаленном режиме). Это означает, что информация заказчика передается по внешним (по отношению к заказчику и аутсорсеру) каналам связи и может быть недобросовестно использована или недостаточно хорошо защищена оператором этих каналов. Кроме того, провайдер связи может испытывать технические проблемы, из-за чего доступ заказчика к необходимым ему информационным ресурсам может быть ограничен. Таким образом, мы считаем необходимым учитывать также риски недобросовестной или некачественной работы провайдера интернет-доступа;

L_{out} – размер потерь заказчика от недобросовестного или несанкционированного поведения аутсорсера (т. е. от целенаправленного срыва аутсорсером выполнения своих контрактных обязательств). Нам представляется целесообразным выделить эту категорию возможных потерь заказчика в качестве самостоятельной, поскольку она связана со специфическими рисками аутсорсинга. Примером ситуации, в которой могут возникнуть такие потери заказчика, служит передача аутсорсером полученной им от заказчика информации его конкурентам. Эта вероятность может быть оценена экспертно, кроме того, в настоящее время существуют шкалы для оценки добросовестности аутсорсера. Отметим, что на сегодняшний день при использовании международного ИТ-аутсорсинга для российских предприятий существуют риски включения в санкционные списки США и ЕС, после чего сотрудничество западных контрагентов с этими предприятиями может быть приостановлено (как это произошло при международном аутсорсинге в российской нефтегазовой отрасли). При оценке возможных потерь заказчика от недобросовестного или несанкционированного поведения аутсорсера мы предлагаем учитывать и эти риски;

W_{out} – вероятность недобросовестного или несанкционированного поведения аутсорсера;

$L_{NA,out}$ – размер потерь заказчика из-за ненадлежащего функционирования ИС в случае ее создания и обеспечения функционирования силами аутсорсера;

$W_{NA,out}$ – вероятность ненадлежащего функционирования ИС.

Таким образом, экономический эффект от использования ИТ-аутсорсинга (с учетом требований безопасности) E_S может быть определен по следующей формуле:

$$E_S = F_{own} - F_{out}. \quad (3)$$

Очевидно, что использование ИТ-аутсорсинга целесообразно в том случае, если выполняется условие $E_S > 0$.

Таким образом, алгоритм принятия решения об использовании ИТ-аутсорсинга с учетом требований экономической и информационной безопасности имеет следующий вид:

1. Определяется (по формуле (1)) полная стоимость информационной системы при ее создании и обеспечении функционирования силами предприятия.
2. Определяется (по формуле (2)) полная стоимость информационной системы при ее создании и обеспечении функционирования силами аутсорсера.
3. Рассчитывается (по формуле (3)) экономический эффект от использования ИТ-аутсорсинга.
4. На основе выполнения (или невыполнения) условия $E_S > 0$ принимается решение об использовании ИТ-аутсорсинга (или об отказе от него).

Вероятно, для повышения достоверности расчетов, по формулам (1)–(3) следует оценивать нечеткие значения полной стоимости ИС и нечеткие значения экономического эффекта от использования аутсорсинга (методика таких расчетов применительно к ситуации аутсорсинга предложена в работе [6]).

На практике выполнения условия $E_S > 0$ может быть недостаточно для принятия решения об использовании аутсорсинга, поскольку, во-первых, предприятие может требовать не просто положительного значения экономического эффекта, а превышения некоторого порогового значения $E_{S\min}$ и, во-вторых, предприятию может быть необходимо, чтобы величина затрат на создание и функционирование информационной системы, размер потерь от разнообразных нежелательных ситуаций и вероятность наступления этих ситуаций в случае использования ИТ-аутсорсинга были не больше некоторого порогового значения. Тогда условие $E_S > 0$ заменяется более сложным условием (4)

$$\begin{cases} E_S \geq E_{S\min}; \\ C_{out} \leq C_{out,\max}; \\ W_{out,\text{int}} \leq W_{out,\text{int}}^{\max}; \\ L_{out,\text{int}} \leq W_{out,\text{int}}^{\max}; \\ W_{out,ext} \leq W_{out,ext}^{\max}; \\ L_{out,ext} \leq W_{out,ext}^{\max}; \\ W_{out} \leq W_{out}^{\max}; \\ L_{out} \leq L_{out}^{\max}; \\ W_{NA,out} \leq W_{NA,out}^{\max}; \\ L_{NA,out} \leq W_{NA,out}^{\max}. \end{cases} \quad (4)$$

Условие (4) отражает все потребности предприятия при переходе к ИТ-аутсорсингу.

В ситуации, когда заказчику необходимо выбрать одного из нескольких потенциальных аутсорсеров, наряду с условием (4) следует требовать выполнения условия $E_S \to \max$.

Отличие предлагаемой нами методики от традиционного алгоритма обоснования целесообразности использования ИТ-аутсорсинга заключается в том, что в традиционном алгоритме требуется лишь выполнение условия $C_{own} > C_{out}$, тогда как мы в качестве критерия целесообразности перехода к ИТ-аутсорсингу предлагаем (в базовом варианте) выполнение условия $E_S > 0$ (что равнозначно условию $F_{own} > F_{out}$).

Очевидно, что расчет полной стоимости ИС и оценка целесообразности использования ИТ-аутсорсинга по предложенному нами алгоритму представляют собой достаточно трудоемкий процесс, в силу чего мы рекомендуем наш алгоритм к применению только для крупных предприятий (для которых как выгоды аутсорсинга, так и его риски достаточно велики, что оправдывает применение сложных методик обоснования перехода к ИТ-аутсорсингу). В ситуации, когда риски, связанные с нарушением информационной безопасности, сравнительно невелики, предприятие вполне может использовать традиционный подход (выполнение условия $C_{own} > C_{out}$).

Из формул (1)–(3) очевидно, что переход к ИТ-аутсорсингу с учетом требований информационной безопасности оправдан в трех основных ситуациях:

- при значимом для заказчика снижении полной стоимости ИС, достигнутом за счет как снижения затрат на ее создание и поддержку, так и уменьшения вероятных потерь от ненадлежащего функционирования и использования ИС;

- при значимом для заказчика снижении затрат на создание и поддержку ИС при условии, что уровень безопасности ИС не снижается по сравнению с ее созданием и поддержкой собственными силами заказчика;

- при существенном повышении уровня безопасности ИС, полностью компенсирующем рост затрат на создание и поддержку ИС.

Предложенный нами алгоритм, как было заявлено выше, позволяет учесть не только требования снижения затрат на создание и эксплуатацию ИС, но также и требования экономической и информационной безопасности предприятия. По этой причине, как мы полагаем, этот алгоритм будет представлять интерес как для теоретиков, так и для практических специалистов, работающих в сфере ИТ-аутсорсинга.

4.2. Характеристика затрат на систему информационной безопасности коммерческого предприятия

Основные группы затрат на реализацию ИБ

После того, как уже установлен перечень различных элементов затрат на безопасность, необходимо выявить источники данных о затратах. Такая информация уже может существовать, часть ее достаточно легко получить, в то время как другие данные определить будет значительно труднее, а некоторые могут быть недоступны.

Затраты на контроль

Основной объем затрат составляет оплата труда персонала службы безопасности и прочего персонала предприятия, занятого проверками и испытаниями. Эти затраты могут быть определены весьма точно. Оставшиеся затраты в основном связаны со стоимостью конкретных специальных работ и услуг внешних организаций и материально-техническим обеспечением системы безопасности. Они могут быть определены напрямую, таким образом можно достаточно просто получить точный перечень затрат на контроль.

Внутренние затраты на компенсацию нарушений системы безопасности фирмы

Определение элементов затрат этой группы намного сложнее, но большую часть установить достаточно легко:

• Приобретение последних версий программных средств защиты информации.

• Приобретение технических средств взамен пришедших в негодность.

• Затраты на восстановление баз данных и прочих информационных массивов.

• Затраты на обновление планов обеспечения непрерывности деятельности службы безопасности.

• Затраты на внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности.

Труднее выявить объемы заработной платы и накладных расходов:

• По проведению дополнительных испытаний и проверок технологических информационных систем.

• По утилизации скомпрометированных ресурсов.

• По проведению повторных проверок и испытаний системы защиты информации.

• По проведению мероприятий по контролю достоверности данных, подвергшихся атаке на целостность.

• По проведению расследований нарушений политики безопасности.

Выяснение затрат на эти виды деятельности связано с различными отделами:

• Отделом информационных технологий.

• Контрольно-ревизионным и финансовым отделами.

• Службой безопасности.

Поскольку каждый вовлеченный сотрудник вряд ли в течение всего рабочего дня решает проблемы, связанные только лишь с внутренними потерями от нарушений политики безопасности, оценка потерь должна быть произведена с учетом реально затраченного на эту деятельность времени.

Внешние затраты на компенсацию нарушений политики безопасности

Часть внешних затрат на компенсацию нарушений политики безопасности связана с тем, что были скомпрометированы коммерческие данные партнеров и персональные данные пользователей услуг предприятия. Затраты, связанные с восстановлением доверия, определяются таким же образом, как и в случае внутренних потерь.

Однако существуют и другие затраты, которые определить достаточно сложно. В их числе:

• Затраты на проведение дополнительных исследований и разработку новой рыночной стратегии.

• Потери от снижения приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения.

• Затраты, связанные с ликвидацией «узких мест» в снабжении, производстве и сбыте продукции.

• Потери от компрометации производимой предприятием продукции и снижения цен на нее.

• Возникновение трудностей в приобретении оборудования или технологий, в том числе повышение цен на них, ограничение объема поставок.

Перечисленные затраты могут быть вызваны действиями персонала различных отделов, например проектного, технологического, планово-экономического, юридического, хозяйственного, отдела маркетинга, тарифной политики и ценообразования.

Поскольку сотрудники всех этих отделов вряд ли будут заняты полный рабочий день вопросами внешних потерь, то установление объема затрат необходимо вести с учетом реально затраченного времени.

Один из элементов внешних потерь невозможно точно вычислить – это потери, связанные с подрывом имиджа предприятия, снижением доверия потребителя к продукции и услугам предприятия. Именно по этой причине многие корпорации скрывают, что их сервис небезопасен. Корпорации боятся обнародования такой информации даже больше, чем атаки в той или иной форме. Однако многие предприятия игнорируют эти затраты на основании того, что их нельзя установить с какой-либо степенью точности – они только предположительны.

Затраты на предупредительные мероприятия

Эти затраты, вероятно, наиболее сложно оценить, поскольку предупредительные мероприятия проводятся в разных отделах и затрагивают многие службы. Эти затраты могут появляться на всех этапах жизненного цикла ресурсов информационной среды предприятия:

- Планирования и организации.
- Приобретения и ввода в действие.
- Доставки и поддержки.
- Мониторинга процессов, составляющих информационную технологию.

В дополнение к этому, большинство затрат данной категории связано с работой персонала службы безопасности. Затраты на предупредительные мероприятия в основном включают заработную плату и накладные расходы. Однако точность их определения в большей степени зависит от точности установления времени, затраченного каждым сотрудником в отдельности.

Некоторые предупредительные затраты легко выявить напрямую. Они, в частности, могут включать оплату различных работ сторонних организаций, например:

- Обслуживание и настройку программно-технических средств защиты, операционных систем и используемого сетевого оборудования.
- Проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, средств вычислительной техники и т. п.

- Доставку конфиденциальной информации.
- Консультации.
- Курсы обучения.

Источники сведений о затратах

При определении затрат на обеспечение ИБ необходимо помнить, что:

- Затраты на приобретение и ввод в действие программно-технических средств могут быть получены из анализа накладных, записей в складской документации и т. п.
- Выплаты персоналу могут быть взяты из ведомостей.
- Объемы выплат заработной платы должны быть взяты с учетом реально затраченного времени на проведение работ по обеспечению информационной безопасности. Если только часть времени сотрудника затрачивается на деятельность по обеспечению информационной безопасности, то целесообразность оценки каждой из составляющих затрат его времени не должна подвергаться сомнению.
- Классификация затрат на безопасность и распределение их по элементам должны стать частью повседневной работы внутри предприятия. С этой целью персоналу должны быть хорошо известны различные элементы затрат и соответствующие им коды.

Если все элементы собраны и распределены с достаточной точностью, то последующий анализ затрат на безопасность может вылиться лишь в интерпретацию данных.

Примерный перечень затрат коммерческого предприятия на обеспечение ИБ

Предположим, что основы политики безопасности на предприятии сформированы. Систематические затраты на ИБ можно разбить на следующие группы.

Затраты на обслуживание системы безопасности (затраты на предупредительные мероприятия)

Управление системой защиты информации:

- Затраты на планирование системы защиты информации предприятия.
- Затраты на изучение возможностей информационной инфраструктуры предприятия по обеспечению безопасности информации ограниченного распространения.
- Затраты на осуществление технической поддержки производственного персонала при внедрении средств защиты и процедур, а также планов по защите информации.
- Проверка сотрудников на лояльность, выявление угроз безопасности.

• Организация системы допуска исполнителей и сотрудников конфиденциального делопроизводства с соответствующими штатами и оргтехникой.

Регламентное обслуживание средств защиты информации:

• Затраты, связанные с обслуживанием и настройкой программно-технических средств защиты, операционных систем и используемого сетевого оборудования.

• Затраты, связанные с организацией сетевого взаимодействия и безопасного использования информационных систем.

• Затраты на поддержание системы резервного копирования и ведение архива данных.

• Проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, средств вычислительной техники и т. п.

Аудит системы безопасности:

• Затраты на контроль изменений состояния информационной среды предприятия.

• Затраты на систему контроля за действиями исполнителей.

Обеспечение должного качества информационных технологий:

• Затраты на обеспечение соответствия требованиям качества информационных технологий, в том числе анализ возможных негативных аспектов информационных технологий, которые влияют на целостность и доступность информации.

• Затраты на доставку (обмен) конфиденциальной информации.

• Удовлетворение субъективных требований пользователей: стиль, удобство интерфейсов и др.

Обеспечение требований стандартов:

• Затраты на обеспечение соответствия принятым стандартам и требованиям достоверности информации, действенности средств защиты.

Обучение персонала:

• Повышение квалификации сотрудников предприятия в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности.

• Развитие нормативной базы службы безопасности.

Затраты на контроль:

• Плановые проверки и испытания.

• Затраты на проверки и испытания программно-технических средств защиты информации.

• Затраты на проверку навыков эксплуатации средств защиты персоналом предприятия.

• Затраты на обеспечение работы лиц, ответственных за реализацию конкретных процедур безопасности по подразделениям.

• Оплата работ по контролю правильности ввода данных в прикладные системы.

• Оплата инспекторов по контролю требований, предъявляемых к защитным средствам при разработке любых систем (контроль выполняется на стадии проектирования и спецификации требований).

Внеплановые проверки и испытания:

• Оплата работы испытательного персонала специализированных организаций.

• Обеспечение испытательного персонала (внутреннего и внешнего) материально-техническими средствами.

Контроль за соблюдением политики ИБ:

• Затраты на контроль реализации функций, обеспечивающих управление защитой коммерческой тайны.

• Затраты на организацию временного взаимодействия и координации между подразделениями для решения повседневных конкретных задач.

• Затраты на проведение аудита безопасности по каждой автоматизированной информационной системе, выделенной в информационной среде предприятия.

• Материально-техническое обеспечение системы контроля доступа к объектам и ресурсам предприятия.

Затраты на внешний аудит:

• Затраты на контрольно-проверочные мероприятия, связанные с лицензионно-разрешительной деятельностью в сфере защиты информации.

Пересмотр политики информационной безопасности предприятия (проводится периодически):

• Затраты на идентификацию угроз безопасности.

• Затраты на поиск уязвимостей системы защиты информации.

• Оплата работы специалистов, выполняющих работы по определению возможного ущерба и переоценке степени риска.

Затраты на ликвидацию последствий нарушения режима ИБ:

• Восстановление системы безопасности до соответствия требованиям политики безопасности.

• Установка патчей или приобретение последних версий программных средств защиты информации.

• Приобретение технических средств взамен пришедших в негодность.

• Проведение дополнительных испытаний и проверок технологических информационных систем.

• Затраты на утилизацию скомпрометированных ресурсов.

Восстановление информационных ресурсов предприятия:

• Затраты на восстановление баз данных и прочих информационных массивов.

• Затраты на проведение мероприятий по контролю достоверности данных, подвергшихся атаке на целостность.

Затраты на выявление причин нарушения политики безопасности:

• Затраты на проведение расследований нарушений политики безопасности (сбор данных о способах совершения, механизме и способах сокрытия неправомерного деяния, поиск следов, орудий и предметов посягательства; выявление мотивов неправомерных действий и т. д.).

• Затраты на обновление планов обеспечения непрерывности деятельности службы безопасности.

Затраты на переделки:

• Затраты на внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности.

• Затраты на повторные проверки и испытания системы защиты информации.

Внешние затраты на ликвидацию последствий нарушения политики безопасности:

• Обязательства перед государством и партнерами.

• Затраты на юридические споры и выплаты компенсаций.

• Потери в результате разрыва деловых отношений с партнерами.

Потеря новаторства:

• Затраты на проведение дополнительных исследований и разработки новой рыночной стратегии.

• Отказ от организационных, научно-технических или коммерческих решений, ставших неэффективными в результате утечки сведений, и затраты на разработку новых средств ведения конкурентной борьбы.

• Потери от снижения приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения.

Прочие затраты:

• Заработная плата секретарей и служащих, организационные и прочие расходы, которые непосредственно связаны с предупредительными мероприятиями.

• Другие виды возможного ущерба предприятию, в том числе связанные с невозможностью выполнения функциональных задач, определенных его Уставом.

Методика расчета затрат на создание и эксплуатацию системы информационной безопасности

Далее, для экономической оценки комплекса средств защиты, необходимо оценить эффективность его функционирования, сопоставляя затраты на создание системы и результаты, полученные от ее эксплуатации.

Показатели экономической эффективности для различных вариантов организации комплексной защиты информации на предприятии могут быть положены в основу выбора оптимального варианта, так как требуется не только обеспечить информационную безопасность предприятия любыми средствами, но и разумно увеличивать дополнительные расходы на эти цели.

Капитальные затраты в сфере защиты информации представляют собой затраты на организацию и функционирование соответствующих служб и подразделений по защите информации. Эти затраты носят разовый характер и направляются в основные и оборотные средства, т. е. в средства производства услуг по защите информации.

Свою стоимость они переносят на продукцию по частям за счет амортизационных отчислений. Капитальными их называют потому, что они не утрачиваются, а воспроизводятся.

Применительно к системам защиты информации капитальные затраты можно сгруппировать следующим образом:

$$К = К_{пр} + К_{тс} + К_{лс} + К_{по} + К_{ио} + К_{уч} + К_{во} + К_{пл} + К_{оэ},$$

где $К_{пр}$ – затраты на проектирование;

$К_{тс}$ – затраты на технические средства защиты;

$К_{лс}$ – затраты на создание линий связи локальных сетей;

$К_{по}$ – затраты на программное обеспечение;

$К_{ио}$ – затраты на формирование информационной базы;

$К_{уч}$ – затраты на обучение персонала;

$К_{во}$ – затраты на вспомогательное оборудование (устройства пожаротушения, источники бесперебойного питания и др.);

$К_{пл}$ – затраты на производственную площадь;

$К_{оэ}$ – затраты на опытную эксплуатацию.

Затраты на формирование информационной базы $К_{ио}$ относятся к условно-постоянной информации.

Состав затрат на опытную эксплуатацию соответствует составу эксплуатационных затрат. Однако эти затраты учитываются как разовые, поскольку временно (в период опытной эксплуатации) работают сразу две системы – базовая и новая система.

Структура единовременных затрат характеризует удельный вес отдельных статей затрат.

Наибольший удельный вес имеют следующие составляющие: $К_{тс}$, $К_{пр}$, $К_{по}$. Иногда бывает нужно привести разновременные затраты к году внедрения системы защиты информации. Такая проблема возникает, если создание системы длится несколько лет, в соответствии с формулой сложных процентов:

$$K = \sum_{t=1}^{T} K_t(1+E)^{T-1},$$

где $К_t$ – капитальные вложения в год *t*, отсчитываемый от начального момента разработки системы;

Т – год приведения затрат (год внедрения).

Эксплуатационные затраты, в отличие от единовременных, являются повторяющимися. Они повторяются в каждом цикле производства, а рассчитываются в сумме за год. Эксплуатационные затраты осуществляются синхронно с производством. Эксплуатационные затраты составляют часть себестоимости продукции или услуг.

В состав эксплуатационных затрат на систему защиты информации входят следующие затраты:

С = Сзп + Сао + Сто + Слс + Сивц + Сни + Сэл + Спр,

где Сзп – зарплата управленческого персонала, работающего с использованием информационных технологий;

Сао – амортизационные отчисления;

Сто – затраты на техническое обслуживание;

Слс – аренда линий связи (глобальных вычислительных сетей);

Сивц – аренда машинного времени внешнего информационно-вычислительного центра, который осуществляет обслуживание информационной системы данного предприятия;

Сни – затраты на носители информации;

Сэл – затраты на электроэнергию;

Спр – прочие затраты.

Наибольший удельный вес в эксплуатационных затратах принадлежит:

- заработной плате;
- амортизационным отчислениям;
- техническому обслуживанию.

В качестве экономического эффекта от применения средств защиты информации может выступать величина возможного ущерба от последствий компьютерных нарушений.

Ущерб в этом смысле определяется стоимостью всех утраченных технических и программных средств и живого труда, необходимого для ремонта, настройки, восстановления работоспособности системы.

Кроме того, стоимость вышеприведенного ущерба может быть откорректирована с учетом простоев других пользователей и долгосрочных последствий компьютерных нарушений, а также частоты возникновения ущерба.

Приближенно оценка частоты нарушений (интенсивность нарушений) может быть представлена следующей зависимостью:

$$\lambda_{ср} = \frac{N}{n \cdot t},$$

где N – среднее количество нарушений на некотором интервале времени;

t – величина интервала (месяц, год);

n – количество рабочих мест пользователей.

Эффективность комплекса средств защиты информации может быть определена следующим образом:

$$E = \frac{Э}{K},$$

где $Э$ – экономия от предотвращенного ущерба от компьютерных правонарушений;

K – затраты, имеющие место при использовании комплекса средств защиты информации.

Разумеется, без капитальных вложений в использование в производстве информационных технологий не обойтись ни одной фирме, которая хотела бы информационное преимущество перед конкурентами превратить в экономическое.

Эффективность затрат в условиях рыночной экономики может быть определена из уравнения

$$\sum_{i=1}^{N}(B_i - C_i - K_i) \times \frac{1}{(1+\frac{r}{100\%})^{i-ip}} = 0, \qquad (5)$$

где B_i – стоимостная оценка результатов использования средств защиты информации на предприятии;

C_i – дополнительные эксплуатационные издержки (расходы) при внедрении средств защиты в i-м периоде, ден. ед.;

K_i – единовременные капитальные затраты в i-м периоде (году), ден. ед.;

N – число расчетных периодов (лет);

i_p – номер периода (года) получения результатов от применения сетевых технологий;

r – расчетная процентная ставка, ставка дисконта для периода (года), %.

Определив или задав величины B_i, C_i, K_i, N, можно рассчитать оценку эффективности применения средств защиты информации, которая будет определяться величиной r.

Уравнение (5) можно заменить неравенством

$$\sum_{i=1}^{N}(B_i - C_i - K_i) \times \frac{1}{(1-\frac{r_n}{100\%})^{i-ip}} > 0, \qquad (6)$$

где r_n – нормативное значение процентной ставки (показателя эффективности).

Если неравенство (6) соблюдается, то вкладывать средства в использование средств защиты целесообразно.

Оценка эффективности будет более точной, если в уравнение (5) ввести коэффициенты, учитывающие налоги на прибыль и инфляцию.

Таким образом, для определения экономической эффективности необходимо определить основные статьи затрат и снижения расходов за счет использования средств защиты информации.

4.3. Совокупная стоимость владения системой информационной безопасности

В настоящее время в отечественных информационных системах (ИС) с повышенными требованиями в области информационной безопасности (ИБ) (банковские системы, производственные предприятия, и т. п.) затраты на обеспечение режима ИБ составляют до 30% всех затрат на ИС.

Информационной безопасности в компании можно не уделять никакого внимания, и не исключен такой вариант, что принятый риск себя вполне оправдает. Можно потратить на создание корпоративной системы защиты информации много денег, и при этом останется некоторая уязвимость, которая рано или поздно приведет к утечке или хищению конфиденциальной информации и к достаточно большому ущербу.

Эксперты-практики в области защиты информации считают, что стоимость системы ИБ должна составлять примерно 10–20% от стоимости КИС, в зависимости от конкретных требований к политике информационной безопасности.

Методика расчета совокупной стоимости владения (ССВ) позволяет рассчитать всю расходную часть информационных активов компании, включая прямые и косвенные затраты на аппаратно-программные средства, организационные мероприятия, обучение и повышение квалификации сотрудников компании, реорганизацию, реструктуризацию бизнеса и т. д.

Показатель ССВ можно использовать как инструмент для оптимизации расходов на обеспечение требуемого уровня защищенности и обоснование бюджета на ИБ.

Основной целью расчета ССВ является выявление избыточных статей расхода. Полученные данные по совокупной стоимости владения используются для выявления расходной части использования корпоративной системы защиты информации.

При определении ССВ необходимо выявить составляющие совокупной стоимости владения и дать их количественную оценку. Все составляющие условно разделяются на единовременные и эксплуатационные. При этом единовременная часть ССВ составляет 25–35%, а эксплуатационная – 75–65%.

Перечень единовременных затрат на формирование системы информационной безопасности приведен выше. Эти затраты носят разовый характер и направляются в основные и оборотные средства для производства услуг по защите информации.

Там же дается перечень эксплуатационных затрат (С), которые повторяются в каждом цикле производства, но рассчитываются в сумме за год. Они составляют себестоимость услуг по защите информации.

Под показателем ССВ понимается сумма прямых и косвенных затрат на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течение года.

При этом прямые затраты включают как капитальные компоненты затрат (ассоциируемые с фиксированными активами или «собственностью»), так и трудозатраты, которые учитываются в категориях операций и административного управления. Сюда же относят затраты на услуги удаленных пользователей и др., связанные с поддержкой деятельности организации.

В свою очередь, косвенные затраты отражают затраты на операции и поддержку (не относящиеся к прямым затратам). Очень часто косвенные затраты играют значительную роль.

Для окончательного расчета величины ССВ необходимо определить проектируемый срок службы системы информационной безопасности ($Т_{пр}$), чтобы рассчитать норму амортизации ($Н_а$) капитальных затрат следующим образом:

$$Н_а = \frac{1}{Т_{пр}}$$

Тогда величина ССВ может быть представлена так:

$$ССВ = К \bullet \frac{1}{Т_{пр}}.$$

На рис. 4.1 представлен график, показывающий изменение величины ССВ с нарастающим итогом за проектируемый срок службы.

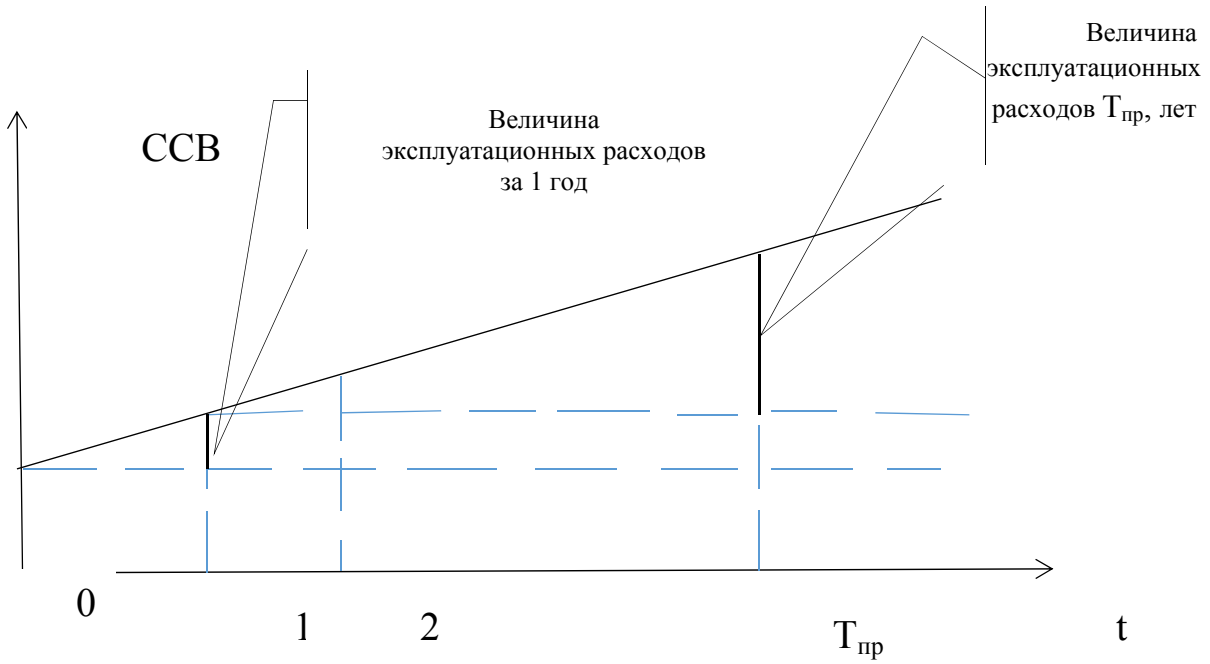


Рис. 4.1. Зависимость величины ССВ от времени нарастающим итогом

Для упрощения предполагается, что ежегодные эксплуатационные расходы равны за весь срок службы.

Анализ затрат по показателю совокупной стоимости владения системами информационной защиты

КОМПАНИЯ № 1

Название: ООО «Компания 1»

Область деятельности: туристический бизнес

Штат сотрудников: 10 человек

Условия: компания оказывает туристические услуги; под офис компания арендует одно из помещений в бизнес-центре. В связи с расширением клиентской базы данных компании руководство решает повысить защищенность информационной системы.

Специфика: 5 ПК, на всех имеется выход в Интернет. Информационная безопасность реализуется штатными средствами операционных систем, СУБД и приложений (парольная защита, разграничение доступа к ресурсам и сервисам) и лицензионными антивирусными средствами. Финансирование ведется в рамках общего ИТ-бюджета.

Уровень зрелости компании с точки зрения ИБ: 0.

Перечень конфиденциальной информации: персональные данные клиентов, сведения о заработной плате сотрудников; информация о договорах с клиентами; личные дела сотрудников; трудовые договоры; бухгалтерская финансовая и налоговая отчетность; внутренние документы, имеющие отношение к информации из перечня защищаемой.

КОМПАНИЯ № 2

Название: ООО «Компания 2»

Область деятельности: охранная деятельность

Штат сотрудников: 30 человек

Условия: компания имеет 2 офиса в бизнес-центре. Обслуживание средств вычислительной техники и защита информации передается на аутсорсинг.

Специфика: 2 стационарных ПК и 1 ноутбук, на всех имеется выход в Интернет, в том числе через VPN. Реализованные средства защиты: разграничение прав доступа штатными средствами операционной системы, лицензионная антивирусная защита, защищенное VPN-соединение.

Уровень зрелости компании с точки зрения ИБ: 0.

Перечень конфиденциальной информации: сведения о заработной плате сотрудников; информация о договорах с заказчиками; личные дела сотрудников; трудовые договоры; журнал регистрации входящих и исходящих документов; бухгалтерская финансовая и налоговая отчетность; стратегия развития предприятия; внутренние документы, имеющие отношение к информации из перечня защищаемой.

КОМПАНИЯ № 3

Название: ООО «Компания 3»

Область деятельности: торговля

Штат сотрудников: 35 человек

Условия: компания имеет 3 розничных магазина, под офис специально оборудовано помещение в одном из магазинов. В связи с увеличением числа клиентов и годового оборота компания открывает еще 2 розничных магазина. Руководство принимает решение об улучшении защиты конфиденциальной информации.

Специфика: 7 ПК, на всех имеется выход в Интернет. Информационная безопасность реализуется штатными средствами операционных систем, СУБД и приложений (парольная защита, разграничение доступа к ресурсам и сервисам) и лицензионными антивирусными средствами. Финансирование ведется в рамках общего ИТ-бюджета

Уровень зрелости компании с точки зрения ИБ: 0.

Перечень конфиденциальной информации: сведения о заработной плате сотрудников; личные дела сотрудников; планы развития Компании; сведения о товарообороте и прибыли; бухгалтерские и финансовые сведения; сведения о фактической себестоимости продукции; схемы, суммы и объемы наличной оплаты товара клиентами; каналы, методы и политика сбыта; клиентская база; сведения о составе торговых агентов и представителей; информация по закупкам, сведения о поставщиках и условиях работы с ними; ценовая политика, стратегия цен; информация о выпуске в

продажу новых товаров; товарные запасы; стратегия и программа рекламных мероприятий; сведения об управлении Компанией.

Данные по ССВ для различных предприятий малого бизнеса сведены в табл. 4.1.

По критерию ССВ для предприятия малого бизнеса целесообразнее привлекать аутсорсинговую компанию для защиты информационных активов, так как «Компания 1» несет самые большие издержки.

Преимущества аутсорсинга ИБ:

- возможность реализации круглосуточного мониторинга;
- решение проблемы отсутствия у сотрудников организации требуемой квалификации и опыта;
- решение проблемы возложения на штатных сотрудников дополнительного объема работ;
- в некоторых случаях: сокращение затрат на защиту информации;
- прозрачность и управляемость защитой.

Недостатки аутсорсинга ИБ:

- угроза утечки конфиденциальных данных (решается соответствующими договорными отношениями);
- возможность потери контроля.

Данные расчета ССВ позволят:

• Получить адекватную информацию об уровне защищенности вычислительной среды и совокупной стоимости владения корпоративной системой защиты информации.

• Сравнить подразделения службы ИБ компании как между собой, так и с аналогичными подразделениями других предприятий в данной отрасли.

• Оптимизировать инвестиции на ИБ компании с учетом реального значения величины ССВ.

Показатель ССВ может использоваться практически на всех основных этапах жизненного цикла корпоративной системы защиты информации.

Сравнение определенного показателя ССВ с аналогичными показателями ССВ по отрасли (с аналогичными компаниями) и с «лучшими в группе» позволяет объективно и независимо обосновать затраты компании на ИБ. Ведь часто оказывается довольно трудно или даже практически невозможно оценить прямой экономический эффект от затрат на ИБ. Сравнение же «родственных» показателей ССВ позволяет убедиться в том, что проект создания или реорганизации корпоративной системы защиты информации компании является оптимальным по сравнению с некоторым среднестатистическим проектом в области защиты информации по отрасли.

Таблица 4.1

Данные по ССВ для различных предприятий малого бизнеса

Наименование товара/услуги	ЗАТРАТЫ, руб.					
	КОМПАНИЯ 1		КОМПАНИЯ 2		КОМПАНИЯ 3	
	единовременные	ежегодные	единовременные	ежегодные	единовременные	ежегодные
Аудит				1800		
Профилактические мероприятия		36000		28800		35800
Регламентный контроль состояния системы защиты				43200		
Поддержание программно-аппаратных средств защиты информации в актуальном состоянии		480000		48000		360000 (специалист по ИБ)
Экстренный вызов специалиста по защите			2000			
Затраты на приобретение и установку антивирусных средств защиты	5750					
Затраты на приобретение и установку комплекса для защиты рабочих станций от интернет-угроз					13500	
ИТОГО	5750	516000	2000	138000	13500	395800
ССВ	521750		140000		409300	

Библиографический список

1. *Аалдерс Р.* ИТ аутсорсинг. Практическое руководство. – М.: Альпина Бизнес Букс, 2004. – 300 с.
2. *Аникин Б.А.*, *Рудая И.Л.* Аутсорсинг и аутстаффинг: высокие технологии менеджмента: Учебное пособие. – М.: ИНФРА-М, 2009. – 320 с.
3. *Бугорский В.Н.*, *Стельмашонок Е.В.* Экономические проблемы информационной безопасности: новый взгляд // Вестник ИНЖЭКОНа. Серия: Экономика. – 2013. – № 1. – С. 67-71.
4. *Васильева И.Н.*, *Стельмашонок Е.В.* Современный взгляд на управление информационной безопасностью предприятия // Вестник ИНЖЭКОНа. Серия: Экономика. – 2014. – № 1. – С. 166-171.
5. *Грошков Д.В.* Оценка рисков поставщика вещевого имущества для нужд Вооруженных Сил // Экономика и предпринимательство. – 2013. – № 11. – С. 490-493.
6. *Давыдкин Е.В.*, *Назаров Д.М.* Оценка эффективности передачи бизнес-процесса на аутсорсинг // Известия Уральского государственного экономического университета. – 2011. – № 4. – С. 62-69.
7. *Котляров И.Д.* Алгоритм отбора аутсорсеров по критерию способности обеспечить целевые значения показателей, описывающих передаваемый процесс // Проблемы экономики и управления нефтегазовым комплексом. – 2012. – № 10. – С. 50-54.
8. *Котляров И.Д.* Оценка рисков сотрудничества с аутсорсером // Проблемы экономики и управления нефтегазовым комплексом. – 2012. – № 11. – С. 34-37.
9. *Котляров И.Д.* Сервисный рычаг и обеспечение доступа к производственным активам предприятия // Вестник НГУЭУ. – 2014. – № 4. – С. 164-172.
10. *Котляров И.Д.* Формализация задачи распределения функций между различными аутсорсерами // Анализ, моделирование, управление, развитие социально-экономических систем: сборник научных трудов IX Международной школы-симпозиума АМУР-2015, Севастополь, 12–21 сентября 2015 г. / Под ред. доц. А.В. Сигала. – Симферополь: КФУ имени В.И. Вернадского, 2015. – С. 174-176.
11. *Тушавин В.А.* Управление качеством ИТ-процессов производственного предприятия. – М.: Научные технологии, 2015. – 249 с.

4.4. Проблемы обеспечения экономической безопасности России на основе повышения качества жизни ее населения

В современных условиях, когда ситуация в мировом сообществе характеризуется переходом к инновационному росту экономик, Россия тоже взяла курс на новую «эру качества и информатизации экономики», свя-

занную с экономической и информационной безопасностью как частью национальной безопасности страны. В рамках Концепции долгосрочного социально-экономического развития и Стратегии национальной безопасности страны особое внимание уделено экономической безопасности через механизмы защиты информационных ресурсов страны от угроз и рисков любого характера и совершенствование социальной политики в части повышения качества жизни населения [19, 27].

Повышение качества жизни является важнейшей составной частью экономической и национальной безопасности РФ, обеспечивает поддержание социально-экономической стабильности в обществе и нуждается в системном исследовании и мониторинге динамики основных социально-экономических показателей развития регионов и составлении рейтингов качества жизни, которые невозможно осуществить без современных инфокоммуникативных технологий, требующих защиты.

В результате, с развитием современных информационных технологий и изменением современного мирового сообщества, рост качества жизни выступает как ведущий фактор преобразований в социальной инфраструктуре и роста благосостояния населения, как инструмент, способствующий раскрытию человеческих ресурсов и возможностей, что в совокупности ведет к развитию инновационной экономики.

Для того чтобы защитить информационные ресурсы страны, необходимо их описать и оценить. Для принятия обоснованных решений в рамках нижеперечисленных проблем необходима инструментальная поддержка в виде комплекса информационных систем и технологий, экономико-математических моделей анализа и прогнозирования качества жизни населения.

Повышение качества жизни населения в регионах невозможно без решения следующих *проблем:*

1) защиты информационных ресурсов страны от угроз и рисков любого характера;

2) разработки системы показателей, всесторонне характеризующих качество жизни населения в регионах;

3) мониторинга и анализа динамики качества жизни населения в регионах;

4) выявления закономерностей изменения качества жизни в регионах;

5) выявления факторов, влияющих на изменение качества жизни в регионах;

6) анализа дифференциации качества жизни по регионам, социально-демографическим группам населения;

7) оценки степени удовлетворения потребностей населения в регионах в материальных благах и услугах по сравнению с рациональными нормами их потребления;

8) разработки обобщающих показателей качества жизни в регионах;

9) совершенствования системы источников данных для анализа качества жизни населения в регионах: материалы переписей и выборочных социально-демографических обследований; бюджеты домашних хозяйств; материалы специальных обследований (в первую очередь социологических);

10) совершенствования национальной системы защиты прав человека путем развития судебной системы и законодательства;

11) содействия росту благосостояния, сокращению бедности и различий в уровне доходов населения в интересах обеспечения постоянного доступа всех категорий граждан к необходимому для здорового образа жизни количеству пищевых продуктов;

12) создания условий для ведения здорового образа жизни, стимулирования рождаемости и снижения смертности населения;

13) развития транспортной инфраструктуры;

14) совершенствования системы защиты от безработицы, создания условий для вовлечения в трудовую деятельность людей с ограниченными физическими возможностями, проведения рациональной региональной миграционной политики, развития пенсионной системы, внедрения нормы социальной поддержки отдельных категорий граждан;

15) обеспечения сохранности культурного и духовного наследия, доступности информационных технологий, а также информации по различным вопросам социально-политической, экономической и духовной жизни общества;

16) совершенствования государственно-частного партнерства в целях укрепления материально-технической базы учреждений здравоохранения, культуры, образования, развития жилищного строительства и повышения качества жилищно-коммунального обслуживания;

17) обеспечения продовольственной безопасности за счет развития биотехнологий и импортозамещения по основным продуктам питания, а также путем предотвращения истощения земельных ресурсов и сокращения сельскохозяйственных земель и пахотных угодий, захвата национального зернового рынка иностранными компаниями, бесконтрольного распространения пищевой продукции, полученной из генетически модифицированных растений с использованием генетически модифицированных микроорганизмов и микроорганизмов, имеющих генетически модифицированные аналоги;

18) защиты населения от чрезвычайных ситуаций природного и техногенного характера.

Необходимо проведение исследований по оценке информативности индикаторов качества жизни населения, нужна разработка моделей прогнозирования на основе международных индексов и статистической оценки различных социально-экономических индикаторов развития регионов и составления на их основе долгосрочных прогнозов.

Традиционные модели в ряде случаев малоинформативны, а доступность информации по качеству жизни ограничена или показатели разработаны относительно недавно и нет многолетней статистики. До настоящего времени не существует объективных критериев для составления страновых прогнозов качества жизни населения.

Поскольку результаты, полученные по итогам расчетов международных индексов, сильно отличаются от используемых методик, то полезные результаты может принести сопоставление международных индексов отдельной страны в динамике за несколько лет и составление прогнозов на основе эконометрических моделей. Межстрановое сопоставление рекомендуется проводить по результатам эконометрического моделирования на основе собранных панельных данных. В качестве факторов могут быть использованы основные международные индексы [1].

Основная проблема моделирования уровня качества жизни населения заключается в неоднородности факторов, влияющих на уровень качества жизни. Все индикаторы и рейтинги предполагают сложные процедуры вычислений, субъективны, плохо комбинируются друг с другом, сложны в интерпретации. Необходимы универсальные процедуры, методы и модели оценки качества жизни, исключающие вышеперечисленные недостатки.

Федеральной целевой программы повышения качества жизни населения страны не существует. Вместо нее – в структуре расходов федерального бюджета по направлению «Новое качество жизни» прописаны основные 12 программ: развитие здравоохранения; развитие образования; социальная поддержка граждан; доступная среда, как обеспечение доступным и комфортным жильем и коммунальными услугами граждан Российской Федерации; содействие занятости населения; обеспечение общественного порядка и противодействие преступности; противодействие незаконному обороту наркотиков; защита населения и территорий от чрезвычайных ситуаций; обеспечение пожарной безопасности и безопасности людей на водных объектах; развитие культуры и туризма; охрана окружающей среды; развитие физической культуры и спорта.

В сторону увеличения изменится доля расходов на реализацию ряда государственных программ: «Социальная поддержка граждан» (с 30,9% в

2014 г. до 34,4% в 2017 г., в связи с преобладанием в программе не подлежащих сокращению расходов на исполнение обязательств по выплате социальных пособий и компенсаций в сфере социальной защиты населения), «Развитие образования» на 2013–2020 гг. (с 13,3% в 2014 г. до 14,8% в 2017 г., определена как приоритетная), «Развитие физической культуры и спорта» (с 1,8% в 2014 г. до 2,8% в 2017 г., в связи с подготовкой к проведению Чемпионата мира по футболу 2018 г. в Российской Федерации) в общем объеме расходов на направление.

Существенно сократится доля расходов федерального бюджета в общем объеме расходов по направлению на реализацию государственных программ «Развитие здравоохранения» (с 10,4 до 7,7%) и «Обеспечение доступным и комфортным жильем и коммунальными услугами граждан Российской Федерации» (с 2,6 до 2,1%). Основными факторами, повлиявшими на снижение объемов бюджетных ассигнований федерального бюджета, являются:

- передача финансового обеспечения медицинских учреждений федерального уровня, оказывающих амбулаторную и стационарную медицинскую помощь (за исключением высокотехнологичной медицинской помощи и подведомственных федеральным органам исполнительной власти, в которых предусмотрена военная служба), в систему обязательного медицинского страхования;

- завершение ряда проектов, в том числе уменьшение расходов федерального бюджета, предоставляемых в виде межбюджетных трансфертов бюджетам субъектов Российской Федерации.

Поэтому необходима разработка моделей оптимизации бюджетного финансирования регионов в соответствии с их потребностями.

Проблема повышения качества жизни населения относится к числу интенсивно исследуемых проблем как в России, так и за рубежом. Эта проблема стала объектом пристального внимания таких авторов, как Л.А. Беляева, С.А. Айвазян, Ю.В. Крупнов, В. Буланова, Е. Катайцева и др., в работах которых рассмотрены различные аспекты повышения качества жизни [10, 12, 14, 15, 21]. Проведенный анализ показал:

- отсутствие в научной литературе единого мнения определения понятия качества жизни, определяющих его факторов, рисков и угроз, методов, моделей и методик его оценки;

- необходимость разработки механизмов повышения качества жизни населения;

- непосредственное влияние повышения качества жизни населения на экономический рост и ускорение развития научно-технического прогресса.

Повышение качества жизни населения РФ и регионов остается одной из главных целей и задач государства. Конституцией РФ в статье 7,

п. 1, политика Российской Федерации как социального государства направлена, в первую очередь, на создание условий, обеспечивающих достойную жизнь и свободное развитие человека. Согласно Конституции Российской Федерации, охраняются труд и здоровье людей, устанавливается гарантированный минимальный размер оплаты труда, обеспечивается государственная поддержка семьи, материнства, отцовства и детства, инвалидов и пожилых граждан, развивается система социальных служб, устанавливаются государственные пенсии, пособия и иные гарантии социальной защиты [2, статья 7, п. 1-2].

Основные направления деятельности Правительства Российской Федерации на период до 2018 г. также определяют цели и стратегии развития в области социального и экономического развития на период до 2018 г., разработанные в соответствии с Федеральным конституциональным законом «О правительстве Российской Федерации» [3].

Механизмы достижения определенного качества жизни населения Российской Федерации устанавливаются в соответствующих программах развития, определяющих условия функционирования экономики страны, ее регионов, условия обеспечения финансовыми ресурсами федерального бюджета и бюджетов субъектов Российской Федерации [3].

Вследствие сильной зависимости от энергосырьевого экспорта, а также высокой степени интеграции российской банковской и финансовой сфер в мировую финансовую систему российская экономика в большей степени, чем экономики других стран, оказалась подвержена воздействию кризисных факторов [3]. Переход к новой модели экономического развития предполагает обеспечение устойчивого и динамичного повышения качества жизни россиян, обеспечение сбалансированного регионального развития, решение демократических, социальных и экологических задач, обеспечение национальной безопасности.

Рекомендовано в [3] в рамках совершенствования инструментов финансовой поддержки регионов установить четкие принципы распределения и предоставления дотаций на поддержку мер по обеспечению сбалансированности бюджетов субъектов Российской Федерации, усилить роль стимулирующих механизмов предоставления финансовой помощи, направленной на повышение уровня социально-экономического развития регионов.

Считаем, что реализация Основных направлений деятельности Правительства Российской Федерации на период до 2018 г. позволит преодолеть ограничения социального и экономического развития и создать условия для устойчивого повышения уровня благосостояния российских граждан и снизить степень конфликтности в социуме. Усилившаяся дифференциация уровня потребления по социальным группам

населения и по регионам заставляет обратиться к проблеме повышения качества жизни населения в регионах РФ [3].

Не во всех регионах удается поддерживать высокий уровень жизни, который является гарантией социальной безопасности и конкурентоспособности всей экономики России в современных условиях. Проблема повышения качества жизни не потеряла своей актуальности и в период глобализации экономик. Страны, которые не сумели создать благоприятные условия для проживания, рискуют утратить социальную стабильность и национальную независимость.

Очевидна масштабность проблемы улучшения качества жизни в России, необходимы меры государственного регулирования социальной политики в регионах и обеспечения конкурентоспособности страны.

К числу таких территориально-хозяйственных образований относится Северо-Западный федеральный округ (СЗФО), образованный Указом Президента РФ в 2000 г., объединивший 7 областей, 2 республики и 1 округ. Административным центром и крупнейшим городом округа является город федерального значения Санкт-Петербург.

Анализ основных социально-экономических показателей развития СЗФО представлен на рис. 4.2.

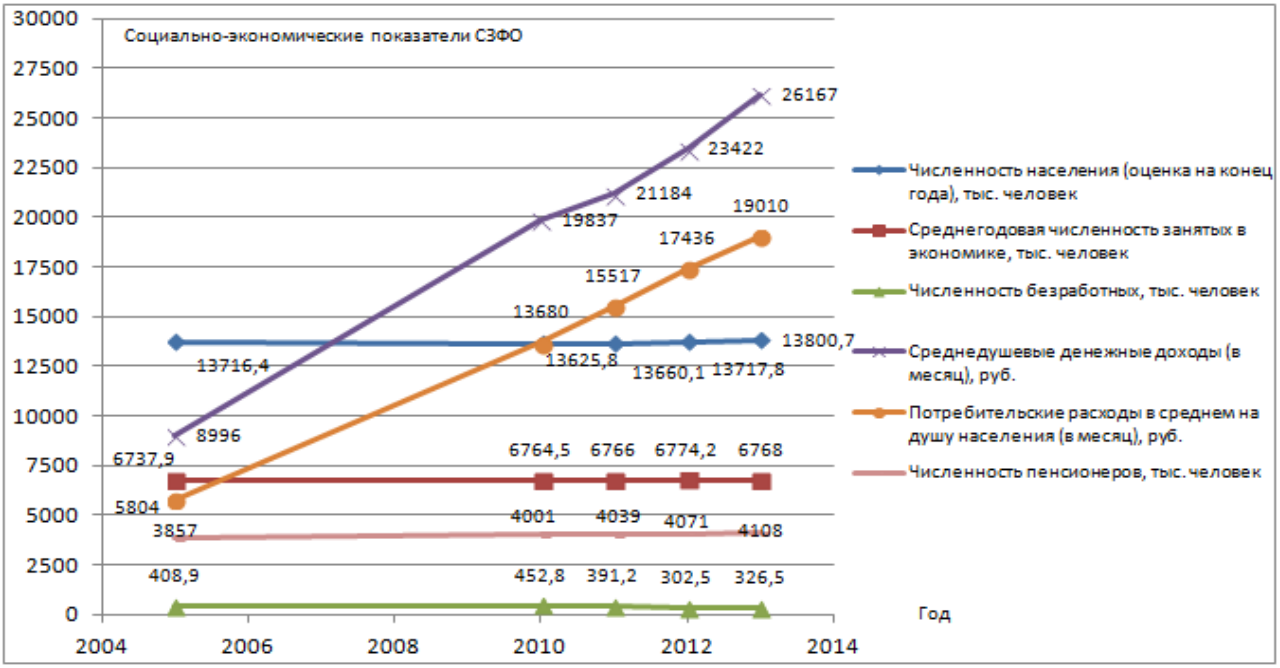


Рис. 4.2. Динамика социально-экономических показателей СЗФО [6, 7]

За период с 2004 по 2013 г. наблюдается среднедушевой рост денежных доходов, потребительских расходов при практически неизменных уровнях остальных индикаторов, что позволило значительно улучшить рейтинг качества жизни населения данного региона (рис. 4.3).

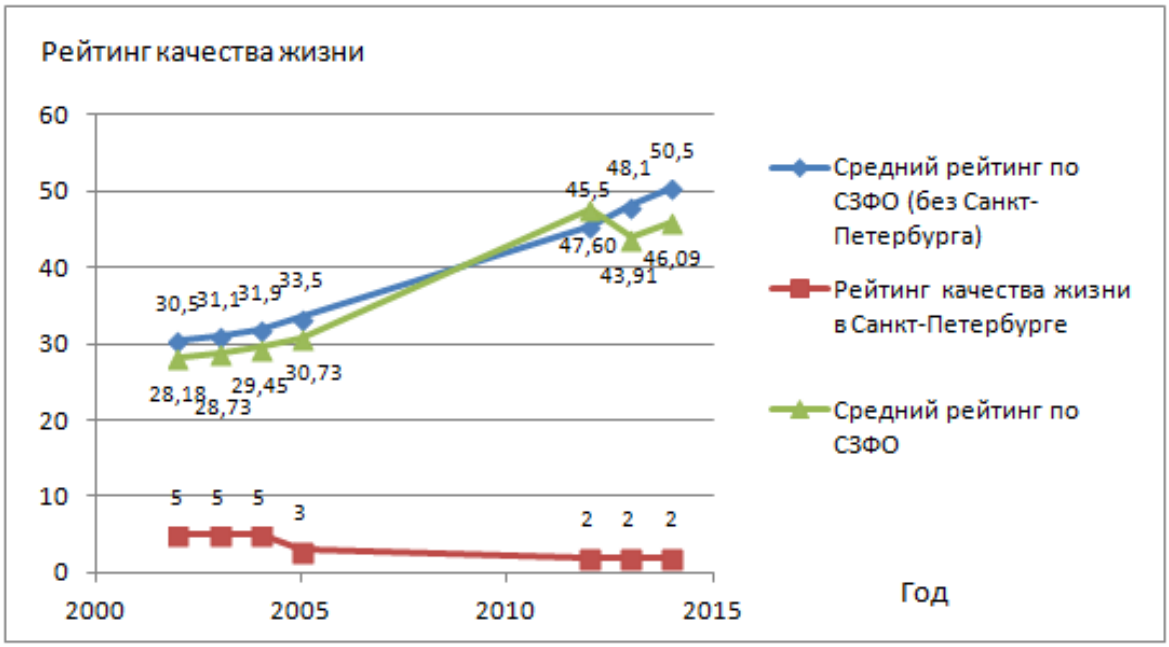


Рис. 4.3. Динамика рейтинга качества жизни в СЗФО [6, 8, 9]

По мнению экспертов Международной Организации Объединенных Наций (ООН), в докладе о человеческом развитии 2014 «Обеспечение устойчивого прогресса человечества: уменьшение уязвимости и формирование жизнестойкости» в рамках программы развития Организации Объединенных Наций (ПРООН) основным показателем человеческого развития является индекс человеческого развития (для России – 0,778) и его компоненты:

-индекс человеческого развития, скорректированный с учетом неравенства (для России – 0,685);

-индекс гендерного неравенства (для России – 0,314);

-индекс гендерного развития (для России – 1,038);

-индекс многомерной бедности (для России – нет данных).

В настоящее время существует множество определений понятий уровня жизни и качества жизни.

Уровень жизни – сложная социально-экономическая категория, ее характеристику можно осуществить с помощью системы показателей. В настоящее время отсутствует единый обобщающий показатель уровня жизни, поскольку не выработано рационального способа объединения многих разноплановых показателей.

В рамках данной работы под *уровнем жизни* населения понимается обеспеченность населения необходимыми материальными благами и услугами, достигнутый уровень их потребления и степень удовлетворения разумных (рациональных) потребностей. Уровень жизни населения зависит от его доходов, социального обеспечения, доступности материальных и духовных благ и услуг.

По мнению Л.А. Беляевой, *качество жизни* населения – объективно-субъективная характеристика условий существования человека, которая зависит от развития потребностей самого человека и его субъективных представлений и оценки своей жизни [10].

Под *качеством жизни* понимается удовлетворенность населения своей жизнью с точки зрения различных потребностей и интересов [1, 11]. Данное понятие включает характеристики и индикаторы уровня жизни, с учетом условий труда и отдыха, жилищных условий, социальной обеспеченности и гарантий, охраны правопорядка и соблюдения прав личности, природно-климатических условий, показателей сохранности окружающей среды, наличия свободного времени и возможности его использовать. Наконец, субъективные ощущения покоя, комфортности и стабильности.

По мнению Ю.В. Крупнова, качество жизни – категория, с помощью которой характеризуют существенные обстоятельства жизни населения, определяющие степень достоинства и свободы личности каждого человека. Качество жизни и уровень жизни не всегда тождественны, поскольку имеют различные жизненные стандарты, критерии и показатели оценки качества жизни [12].

Другие авторы также внесли свой вклад в исследование содержания категории «качество жизни» (табл. 4.2).

Таблица 4.2

Анализ определений «качества» жизни

Автор (страна)	Определение
Ньюэл М. (Великобритания)	Качество жизни (образование, здравоохранение, культура, экология и т. п.) – антитеза уровню жизни
Белл Д. (США)	Качество жизни – цель постиндустриального общества, измеряемая услугами и удобствами для всех
Тодоров А.С. (Болгария)	Качество жизни – социологическая категория, отражающая степень удовлетворения духовных, интеллектуальных, культурных, эстетических и других потребностей людей
Всероссийский центр уровня жизни (Россия)	Качество жизни – сущность развития жизни, социальных групп и всего общества страны в увязке со степенью удовлетворения ими своих потребностей
Всемирная организация здравоохранения (ВОЗ)	Качество жизни – восприятие индивидом своего положения в культурном и ценностном контекстах его жизни, с целями, потребностями и интересами этого индивида
ВНИИТЭ (Россия)	Качество жизни – совокупность жизненных ценностей, характеризующих виды деятельности, структуру потребностей и условия существования человека (групп населения, общества), удовлетворенность людей жизнью, социальными отношениями и окружающей средой

Окончание табл. 4.2

Автор (страна)	Определение
Бестужев-Лада И.В. (СССР)	Качество жизни – непрерывный процесс формирования подлинно человеческого сообщества, предоставляющего личности возможность всестороннего творческого развития
Субетто А.И. (Россия)	Качество жизни – критерий всей государственной внешней и внутренней политики и проводимых реформ
Львов Д.С. (Россия)	Качество жизни общества должно определяться разнообразием жизненных благ, которые могут быть гарантированы каждому его члену
Бойцов Б.В., Крянев Ю.В., Кузнецов М.А. (Россия)	Качество жизни – системно-целостное образование, формируемое через взаимосвязь разнокачественных составляющих, которое приобретает черты целостности и смысловой завершенности под влиянием духовности
Айвазян С.А. (Россия)	Качество жизни – сложная синтетическая категория, аккумулирующая в себе все существенные для личности условия существования и развития
Рыбак А.И., Панафидин Г.С. (Россия)	Качество жизни человека – оценочная категория жизни человека, обобщенно характеризующая параметры всех составляющих его жизни: жизненного потенциала, жизнедеятельности и условий жизнедеятельности по отношению к некоторому объективному или субъективному эталону
Крупнов Ю. В. (Россия)	Качество жизни является главной целевой функцией современных сверхиндустриальных промышленных систем, определяется через интегральные показатели качества жизни. Три блока комплексных индикаторов: - здоровье населения и демографическое благополучие; - удовлетворенность населения индивидуальными условиями жизни; - духовное состояние общества

В настоящее время не существует единого мнения в разделении понятий «уровень жизни» и «качество жизни». Часто они взаимозаменяемы, а перечни показателей во многом совпадают. Согласны с мнением Ю. В. Крупнова, что их следует различать [12] (табл. 4.3). В связи с этим актуальным является вопрос о разработке единого *обобщающего показателя* уровня жизни, позволяющего сравнивать его по странам и регионам. Так как уровень жизни в значительной степени определяется уровнем экономического развития страны, в качестве такого обобщающего показателя часто используют показатель ВВП, национального дохода, чистого располагаемого дохода.

Таблица 4.3

Сравнительный анализ понятий «уровня» и «качества» жизни

«Уровень жизни»	«Качество жизни»
Более узкая категория, чем «качество жизни»	Более широкая категория, включающая в себя уровень жизни
Определяется условиями существования человека в сфере потребления	Определяется широким комплексом условий жизнедеятельности
Измеряется через социально-экономические показатели общего благосостояния людей	Для измерения необходимы субъективные оценки соответствия статистических параметров потребностям людей
Абсолютные показатели: - доходы, - потребление, - жилищные условия, - услуги образования, - услуги здравоохранения и др.	Относительные показатели в сферах: - экологическая, - социальная, - политическая, - психологическая
Характеризует достигнутый уровень обеспеченности населения необходимыми для жизни материальными, духовными и социальными благами	- индивида (продолжительность жизни, продолжительность активной части жизни, уровень физического и психического здоровья, уровень образования, культурного и интеллектуального потенциала), - состояние сферы обитания человека; - экологические параметры обитания, его комфортность, - удобство жизненных условий

В современных исследованиях категория «качество жизни» получило широкое применение как интегральный индикатор, характеризующий уровень экономического развития общества с ориентацией на потребности населения. Выделяют следующие научные подходы к формулированию определения качества жизни: философский, экономический, экологический, психологический, медицинский, социологический, географический, представленные в табл. 4.4.

Таким образом, «качество жизни» рассматривается как междисциплинарная категория, которой свойственны: интегративность, связь с удовлетворенностью жизнедеятельности, связи с культурно-исторической и природно-экологической средами жизни.

Таблица 4.4

Сравнительный анализ
подходов к исследованию определения «качества» жизни

Подход	Определение	Характеристика	Представители
Философский	Удовлетворенность личностью уровнем реализации духовных, культурных потребностей, своей жизнедеятельностью в условиях социума	Связь с духовностью, нравственностью, образованностью, справедливостью, счастьем	А.С. Тодоров
Психологический	Субъективная удовлетворенность человека своей жизнью, которая выражается в оценке уровня и степени реализации своих потребностей	В исследованиях качества жизни необходимо учитывать взаимосвязь объективных условий и их субъективную оценку	Г.М. Головина, Т.Н. Савченко
Экономический	Отражение материального уровня благосостояния субъекта и как способность человека воспроизводить и увеличивать свой материальный достаток	Две точки зрения: -оптимистический: переход к обществу нового качества жизни возможен только на основе научно-технического прогресса; -пессимистический: экономический рост, ухудшая состояние окружающей среды, оказывает отрицательное воздействие на жизнь человека	Р. Арон, Д. Белл, Дж. Гэлбрейт, П. Дракер, Э. Тоффлер, У. Ростоу
Экологический	Совокупность условий, при которых не только не нарушается состояние окружающей среды, но и сохраняются природные ресурсы, необходимые для существования будущих поколений	Экономический рост, не согласованный с законами природы, приведет к исчерпанию ресурсной базы, разрушению природной среды и гибели человечества	У. Бек, Д.М. Гвишиани, В.И. Данилов-Данильян, Н.Н. Моисеев, Н.Ю. Рейменс, Д.Ж. Маркович
Медицинский	Субъективное удовлетворение, испытываемое индивидуумом в физических, ментальных, социальных ситуациях	Сохранение и воспроизводство жизни и здоровья человека, воспроизводство человеческого рода, здорового образа жизни	Р. Джонсен, Н.А. Агаджанян

Окончание табл. 4.4

Подход	Определение	Характеристика	Представители
Социологический	Удовлетворение материальных и духовных потребностей, социальных интересов различных групп людей	Результат комбинаций различных статистических величин: уровня преступности, безработицы, доходов и потребления	Дж. Форрестер, П.А. Сорокин, В.Б. Бойцов
Географический	Характеризует соответствие многокомпонентной системы среды жизни объективным нормам и субъектным потребностям территориальной общности	Зависит от многих факторов и условий жизнедеятельности, а также от субъективного отношения индивида к различным сторонам своей жизни	В.Т. Ганжин

Объектами оценки качества жизни являются критерии и показатели качества жизни, которые можно сгруппировать по принадлежности к материальным и нематериальным компонентам (рис. 4.4).

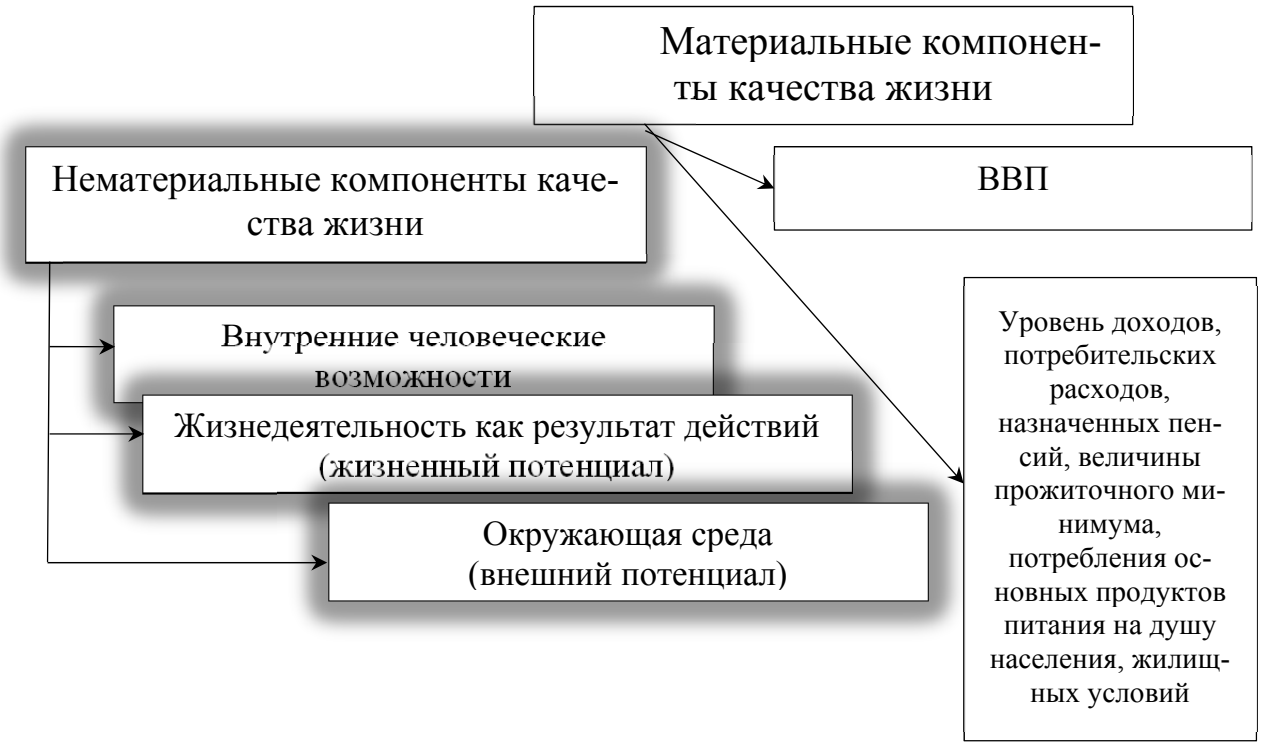


Рис. 4.4. Деление показателей качества жизни на компоненты [13]

Под внутренними человеческими возможностями понимается нематериальный компонент качества жизни, данный определённому человеку (или социуму) – *внутренний потенциал,* позволяющий достигать опреде-

ленного уровня качества жизни (генетика, психофизические возможности, талант и др.).

Жизненный потенциал формируется в течение жизни, а качество жизни как нематериальная характеристика жизнедеятельности определяется способностями достигать намеченных целей в соответствии с имеющимися у людей потребностями, интересами, ценностями.

Окружающая среда формирует *внешний потенциал* и определяет качество жизни: семья, социум, субкультура с использованием возможностей свойств окружающих объектов и субъектов, институциональные условия функционирования экономической системы (политический режим, используемые методы управления институтами, централизация или децентрализация власти и т. д.).

Следует выделить материальные компоненты, оказывающие влияние на качество жизни населения и связанные с материальным благополучием населения (уровень доходов, потребительских расходов, назначенных пенсий, величины прожиточного минимума, потребления основных продуктов питания на душу населения, жилищных условий).

Нематериальные компоненты качества жизни населения [13], используемые в индикаторах качества жизни населения, представлены в табл. 4.5.

Таблица 4.5

Нематериальные компоненты качества жизни населения

Нематериальные компоненты качества жизни	Индикаторы и рейтинги качества жизни населения
Внутренние человеческие возможности (внутренний потенциал)	- Всемирный индекс счастья; - Глобальный индекс миролюбия; - Индекс развития человеческого потенциала; - Индекс удовлетворенности жизнью в странах мира; - Рейтинг стран мира по уровню счастья по версии Gallup
Жизнедеятельность как результат действий (жизненный потенциал)	- Индекс качества жизни пожилых людей; - Рейтинг стран мира по уровню научно-исследовательской активности; - Рейтинг стран мира по уровню образования; - Рейтинг стран мира по уровню защиты прав собственности; - Рейтинг стран мира по уровню терроризма; - Рейтинг стран мира по уровню расходов на НИОКР; - Рейтинг стран мира по уровню развития человеческого капитала; - Рейтинг стран мира по уровню продолжительности жизни; - Рейтинг эффективности национальных систем образования по версии Pearson; - Рейтинг стран мира по уровню преднамеренных убийств; - Рейтинг стран мира по уровню потребления алкоголя; - Рейтинг стран мира по уровню инноваций

Окончание табл. 4.5

Нематериальные компоненты качества жизни	Индикаторы и рейтинги качества жизни населения
Окружающая среда (внешний потенциал)	- Индекс качества жизни в городах мира по версии Mercer; - Индекс продовольственной безопасности; - Индекс хороших стран; - Рейтинг 100 лучших стран мира для жизни; - Рейтинг качества жизни регионов России; - Рейтинг социального самочувствия регионов России; - Рейтинг стран мира по уровню качества жизни; - Рейтинг стран мира по уровню демократии; - Рейтинг стран мира по уровню гражданских свобод; - Рейтинг стран мира по уровню свободы СМИ; - Рейтинг стран мира по уровню социального развития; - Рейтинг стран мира по уровню условий ведения бизнеса; - Рейтинг стран мира по уровню устойчивости общества; - Рейтинг стран мира по уровню экологической эффективности; - Рейтинг стран мира по уровню свободы Интернета; - Рейтинг стран мира по уровню расходов на образование; - Рейтинг стран мира по уровню расходов на здравоохранение; - Рейтинг стран мира по уровню процветания; - Рейтинг стран мира по уровню урбанизации

По методике С.А. Айвазяна [14, 15] иерархическая система статистических показателей и частных критериев качества жизни населения, выглядит следующим образом (табл. 4.6).

Таблица 4.6

Критерии и показатели качества жизни населения

Критерии	Показатели
Качественная структура населения	- свойства воспроизводства физического здоровья; - способность образовывать и сохранять семьи; - уровень образования и культуры; - уровень квалификации
Благосостояние населения	- реальные доходы и расходы; - обеспеченность жильем и собственностью; - обеспеченность мощностями инфраструктуры общества
Качество социальной сферы	- условия труда; - физическая и имущественная безопасность; - характеристики социальной и территориальной подвижности населения; - социально-политическое здоровье

Окончание табл. 4.6

Критерии	Показатели
Качество экологической ниши	- состояние воздушного бассейна; - состояние водного бассейна; - состояние почв; - состояние природных экосистем
Природно-климатические условия	- наличие природно-сырьевых ресурсов; - климатические условия; - частота форс-мажорных природных ситуаций

Всемирной организацией здравоохранения был разработан опросник качества жизни населения ВОЗ (ВОЗКЖ-100) с целью оценки качества жизни населения вне зависимости от экономического, социального, культурного или демографического статуса. Качество жизни человека, по определению ВОЗ, – это степень комфортности человека как внутри себя, так и в окружающей среде, которая определяется влияющими на нее физическими, социальными и эмоциональными факторами жизни [16].

Также существует ряд «социальных индикаторов», используемых для мониторинга динамики социальных явлений совместно с экономическими индикаторами для оценки качества жизни населения. Например, американский социолог К. Ланд выделял три типа «социальных индикаторов» [11]. На наш взгляд, наиболее перспективными являются интегральные индикаторы качества жизни населения с учетом как материального, так и нематериального компонента [1, 7, 17, 18].

Субъектами оценки качества жизни населения являются:

- человек;
- население;
- государство;
- правительство РФ;
- региональные правительства;
- Совет Безопасности РФ;
- федеральные органы исполнительной власти;
- органы исполнительной власти субъектов РФ;
- информационно-аналитические институты РФ;
- международные информационно-аналитические институты.

Цели и задачи субъектов, направленные на повышение качества жизни, отражены на рис. 4.5.

Факторы повышения качества жизни	(Ч)	(Н)	(Г)	(П)	(РП)	(СБ)	(ФОИВ)	(РОИВ)	(ИАИ)	(МИАИ)
Переход на более высокий - инновационный уровень развития										
Снижение социальной дифференциации между группами населения, регионами и странами										
Охрана здоровья граждан РФ всех возрастов										
Улучшение условий труда граждан РФ										
Снижение уровня безработицы										
Снижение социальной напряженности										
Изучение качественной структуры населения										
Изучение благосостояния населения										
Качество социальной сферы										
Качество экологической ниши										
Природно-климатические условия										
Повышение уровня образования и культуры										
Способность образовывать и сохранять семьи										
Повышение уровня квалификации населения										

Рис. 4.5. Цели и задачи субъектов, направленные на повышение качества жизни

Субъектам оценки качества жизни интересны решения по следующим вопросам:

- *человек* (Ч) выступает в роли субъекта оценки качества жизни и заинтересован в защите своего здоровья и благополучия, экологичности природной окружающей среды, в расширении прав, равенстве возможностей и предоставлении свободы выбора вести такую жизнь, которая представляет для него наибольшую ценность, а также иметь возможность реализовывать свой человеческий потенциал и творческие способности;

- *население* (Н) при изучении качества жизни также выступает в роли субъекта и заинтересовано: в пользование благами, обеспечивающими всестороннее развитие человека; в рациональном потреблении, обеспечивающем восстановление физических и интеллектуальных сил, в повышении уровня жизни как приоритетном направлении своего развития;

- *государство* (Г) – государственная политика, направленная на повышение качества жизни граждан Российской Федерации, должна разрабатываться одновременно с государственными прогнозами ее социально-экономического развития;

- *правительство РФ* (П) в тесном взаимодействии с *региональными правительствами* (РП) обеспечивает средствами ФОИВ и РОИВ проведение единой государственной политики в области культуры, науки, образования, здравоохранения, социального обеспечения, экологии; осуществляет меры по обеспечению законности, прав и свобод граждан, по обеспечению государственной безопасности;

- *Совет Безопасности РФ* (СБ) рассматривает в рамках национальной безопасности стратегические вопросы военной и оборонно-

промышленной, международной, экономической, государственной и общественной, антитеррористической, информационной безопасности и готовит рекомендации по выполнению федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации возложенных на них функций в этой сфере деятельности по ее обеспечению.

Реализация Стратегии национальной безопасности Российской Федерации до 2020 г. призвана стать мобилизующим фактором развития национальной экономики, улучшения качества жизни российских граждан [19]. Стратегическими целями обеспечения национальной безопасности в области повышения качества жизни российских граждан являются снижение уровня социального и имущественного неравенства населения, стабилизация его численности в среднесрочной перспективе, а в долгосрочной перспективе – коренное улучшение демографической ситуации. Повышение качества жизни российских граждан гарантируется путем обеспечения личной безопасности, а также доступности комфортного жилья, высококачественных и безопасных товаров и услуг, достойной оплаты активной трудовой деятельности [19];

- *федеральные органы исполнительной власти* (ФОИВ) во взаимодействии *с органами исполнительной власти субъектов РФ* (РОИВ) реализуют с учетом региональных условий единую государственную политику в области обеспечения безопасности РФ, разрабатывают и принимают нормативные правовые акты субъектов Российской Федерации по вопросам обеспечения безопасности, обеспечивают ведение мониторинга состояния безопасности на территории субъектов Российской Федерации. Все вышеперечисленное позволит *в регионах*:

- улучшить благосостояние населения;

- создать условия для динамичного развития импортозамещения;

- прогнозировать и предотвращать возникающие угрозы и риски для экономической безопасности страны, повышать ее конкурентоспособность;

- обеспечить социальную безопасность как важнейшую составную часть национальной безопасности;

- *информационно-аналитические институты РФ* (ИАИ)*:*

Федеральная служба государственной статистики (http://www.gks.ru) обеспечивает информационную поддержку органов власти и управления, средств массовой информации, населения, научной общественности, коммерческих организаций и предпринимателей, международных организаций в объективной и полной статистической информации;

Центр гуманитарных технологий. Информационно-аналитический портал (http://gtmarket.ru) проводит исследования, мероприятия, лекции, стенограммы, интервью; формирует рейтинги, составляет прогнозы;

Независимый институт социальной политики (НИСП). Социальный атлас российских регионов (http://atlas.socpol.ru) осуществляет подготовку и проведение научно-исследовательской работы в сфере социальной политики, поддержку независимых научных исследований в этой области; развитие информационных банков и баз данных (БД исследователей и научных организаций, работающих в сфере социальной политики в России; информационное обеспечение, архивирование данных);

Всероссийский центр исследования общественного мнения (ВЦИОМ) (http://wciom.ru) проводит опросы по заказам федеральных и региональных органов государственной власти, а также электоральные и политические исследования проблем социально-экономического развития, рынка труда, миграции, преодоления бедности;

Российская академия народного хозяйства и государственной службы при Президенте РФ (РАНХиГС) (http://www.ranepa.ru) осуществляет научное и экспертно-аналитическое сопровождение органов государственной власти Российской Федерации;

Федеральное государственное бюджетное научно-исследовательское учреждение «Совет по изучению производительных сил» (http://sops.ru) выполняет фундаментальные и прикладные научные исследования в области стратегического и территориального управления и планирования, развития и размещения производительных сил, социально-экономического развития территорий и региональной политики, развития муниципальных образований, инвестиционной политики, разработки и обоснования крупных инвестиционных проектов и программ с участием государства и частного бизнеса, использования природных ресурсов, экологии, энергоэффективности и энергосбережения, комплексных проблем Мирового океана, международного экономического сотрудничества с целью научного обоснования экономического и социального развития страны, выработки предложений для государственных стратегий, прогнозов, программ развития;

Исследовательский холдинг Ромир (Research Rethink React) (http://www.romir.ru) – российский исследовательский центр, реализующий маркетинговые и социологические исследования, является эксклюзивным представителем в России и СНГ ассоциации Gallup International/WIN, что дает возможность для обмена опытом и технологиями;

- *международные информационно-аналитические институты* (МИАИ):

Организация объединенных наций (ООН) (http://www.un.org) осуществляет международное сотрудничество в сфере разрешения международных проблем экономического, социального, культурного и гуманитарного характера;

Всемирный банк (http://www.worldbank.org) является специализированным учреждением ООН, созданным в целях международного экономического развития и финансовой и технической помощи развивающимся странам по всему миру;

Всемирная организация здравоохранения (ВОЗ) (http://www.who.int/ru) является направляющей и координирующей инстанцией в области здравоохранения в рамках системы ООН при проведении научных исследований в области здравоохранения, установлении норм и стандартов, контроле за ситуацией в области здравоохранения и оценке динамики ее изменения;

Организация экономического сотрудничества и развития (ОЭСР) / Organization for Economic Cooperation and Development (OECD) (http://www.oecdbetterlifeindex.org) способствует экономическому росту стран-членов, развитию мировой торговли на многосторонней, недискриминационной основе в соответствии с международными обязательствами;

Британский исследовательский центр The Economist Intelligence Unit (аналитическое подразделение британского журнала Economist) (http://www.eiu.com) проводит расчеты индекса демократии стран на основе полученных экспертных оценок и результатов опросов общественного мнения из исследуемых стран;

Международный исследовательский центр Gallup International: (http://www.wingia.com) занимается исследованием общественного мнения по проблемам внутренней и внешней политики, считается авторитетным источником информации о состоянии общественного мнения в США и в мире;

Британский исследовательский центр New Economic Foundation (http://www.happyplanetindex.org) измеряет уровень счастья в странах мира, оценивает достижения стран и отдельных регионов мира с точки зрения их способности обеспечить своим жителям счастливую жизнь за счет эффективного использования экономического роста и природных ресурсов;

Американский исследовательский центр The Heritage Foundation совместно с газетой The Wall Street Journal. Фонд наследия (http://www.heritage.org) проводит исследования экономических свобод с учетом доли вмешательства государства в процессы производства, распределения и потребления товаров и услуг.

При разработке Концепции развития РФ [27] в части обеспечения ее национальной безопасности необходимо учитывать риски и угрозы снижения качества жизни населения, их влияние на национальную безопасность РФ. Имеющиеся риски и угрозы целесообразно сгруппировать по типам и представить в виде классификации (рис. 4.6).

Обеспечение *национальной безопасности* связано с преодолением влияния негативных факторов, которые формируют риски и угрозы, ведущие к снижению качества жизни, представленные на рис. 4.6.

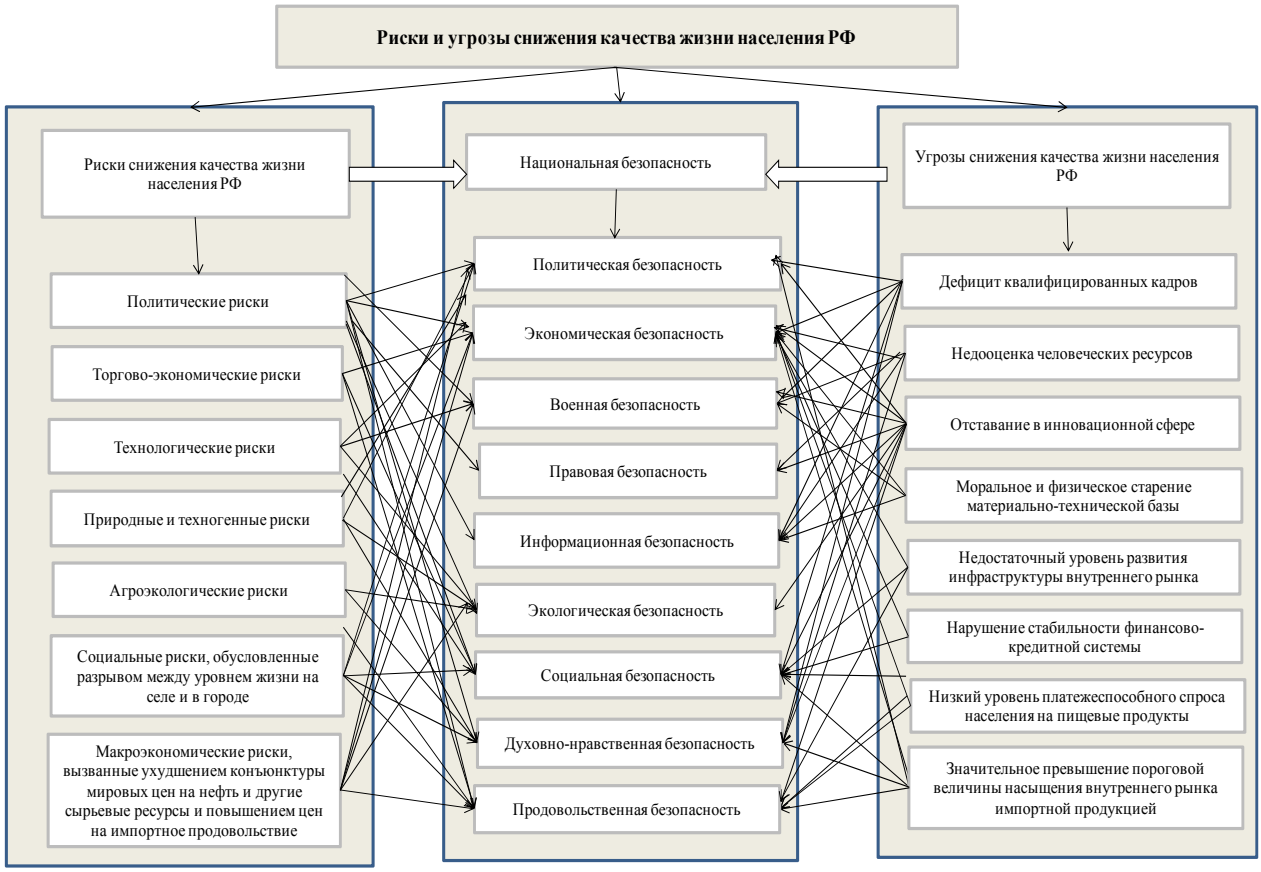


Рис. 4.6. Классификация рисков и угроз снижения качества жизни

Выделенные элементы национальной безопасности на рис. 4.6, согласно [19] (политическая, экономическая, военная, правовая, информационная, экологическая, социальная, духовно-нравственная, продовольственная), напрямую зависят от степени обеспеченности граждан необходимыми для жизни материальными и нематериальными благами, рассчитываемой как соотношение удовлетворенных и желаемых потребностей.

В качестве желаемых потребностей могут выступать пороговые материальные потребности (например, достигнутый уровень потребления человеком того или иного продукта питания, уровень потребления населением материальных благ и услуг в развитых странах, желаемый порог потребления, устанавливаемый на основе научных разработок, медицинских рекомендаций, ориентруясь на уровень среднемесячной заработной платы, минимального размера оплаты труда, объем продовольственной корзины и т. д.).

На первый взгляд, качество жизни населения может считаться достойным и безопасным, если, например, в случае прекращения поступления на территорию страны пищевых продуктов из-за рубежа из-за санкций ЕС и США не возникает продовольственный кризис, что достигается за счет высокой доли в потреблении отечественного сельскохозяйственного сырья и продовольствия, безработицы, финансового кризиса.

Если сопоставить эти ориентиры с тем, что мы имеем сегодня, то наиболее сильно нарушен баланс в обеспечении населения отечественной продукцией животноводства, прежде всего мясной и молочной [28].

Конечно, возрастает влияние на обеспечение качества жизни в России внешних факторов, поскольку продовольствие все больше становится одним из основных факторов политической и социально-экономической стабильности любого государства.

Особенно очевидно это стало в конце 2014 – начале 2015 г., когда на мировых рынках упали цены на нефть, произошла девальвация курса рубля и за этот период цены на продовольствие практически удвоились.

Но нельзя забывать про другие, нематериальные, виды безопасности: духовно-нравственную, правовую, информационную, социальную, политическую, также подверженные влиянию снижения качества жизни населения.

Проблемы обеспечения качества жизни носят многоаспектный, межрегиональный характер, и необходимость их системного решения отражена в Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 г. [27].

Государственная региональная политика направлена на обеспечение сбалансированного социально-экономического развития субъектов Российской Федерации, сокращение уровня межрегиональной дифференциации. Под сбалансированным развитием территорий Российской Федерации понимается обеспечение достойных условий жизни гражданам всех регионов в рамках комплексного развития регионов.

Достижение этой цели будет обеспечено в ходе реализации государственной региональной политики, направленной на реализацию потенциала развития каждого региона, преодоление инфраструктурных и институциональных ограничений, создание равных возможностей граждан и содействие развитию человеческого потенциала, проведение целенаправленной работы по развитию федеративных отношений, а также реформирование систем государственного управления и местного самоуправления.

Библиографический список

1. *Еникеева Л.А.*, *Ширшикова М.С.* Модели прогнозирования качества жизни на основе международных индексов // Современные проблемы науки и образования. – 2015. – № 1 [Электронный ресурс]. – URL: http://www.science-education.ru/121-18414 (дата обращения: 09.04.2015).
2. Конституция Российской Федерации [Электронный ресурс]. – URL: http://graph.garant.ru:8080/SESSION/PILOT/main.htm (дата обращения 15.05.2015).

3. Основные направления деятельности Правительства Российской Федерации на период до 2018 года.
4. Стратегия социально-экономического развития Северо-Западного федерального округа на период до 2020 года [Электронный ресурс]. – URL: http://www.ifap.ru/ofdocs/rus/rus006.pdf (дата обращения 30.03.2015).
5. Интегральные индексы // Социальный атлас российских регионов. [Электронный ресурс]. – URL: http://atlas.socpol.ru/index (дата обращения 23.03.2015).
6. Доклад социально-экономического положения России в 2014 году: РОССТАТ. – 2014 [Электронный ресурс]. – URL: http://www.gks.ru/bgd/regl/b14_01/Main.htm (дата обращения 15.03.2015).
7. Центр гуманитарных технологий – информация об исследованиях [Электронный ресурс]. – URL: http://gtmarket.ru/ (дата обращения 15.03.2015).
8. Проблемы измерения уровня и качества жизни населения [Электронный ресурс]. – URL: http://socialworkstud.ru/ (дата обращения 23.03.2015).
9. Прогнозирование социального развития и уровня жизни населения [Электронный ресурс]. – URL: http://allrefs.net/c3/45ozk/p9/?full (дата обращения 07.04.2015).
10. *Беляева Л.А*. Уровень и качество жизни. Проблемы измерения и интерпретация // Социологические исследования. – 2009. – № 1. – С. 33-42.
11. *Попова С.М*., *Шахрай С.М*., *Яник А.А*. Измерение прогресса / Институт социально-политических исследований РАН. – М.: Наука, 2010. – 272 с.
12. *Крупнов Ю.В*. Качество жизни [Электронный ресурс]. – URL: http://kroupnov.ru/pubs/2005/01/09/10178/ (дата обращения 15.03.2015).
13. *Ширшикова М.С*. Проблемы моделирования качества жизни населения // Научное обозрение. – 2015. – № 7. – С. 382-385.
14. *Айвазян С.А*. Анализ качества и образа жизни населения (эконометрический подход). – М.: Наука, 2012. – 432 с.
15. *Айвазян С.А*. Интегральные индикаторы качества жизни населения: их построение и использование в социально-экономическом управлении и межрегиональных сопоставлениях. – М.: ЦЭМИ РАН, 2000. – 118 с.
16. Опросник качества жизни Всемирной организации здравоохранения (ядерный модуль) // Материалы энциклопедии психодиагностики [Электронный ресурс]. – URL: http://psylab.info/ (дата обращения 15.03.2015).
17. Доклады о развитии человека [Электронный ресурс]. URL: http://www.un.org/ru/development/hdr/ (дата обращения 15.03.2015).

18. *Еникеева Л.А.*, *Ширшикова М.С.* К вопросу об измерении человеческого капитала в контексте анализа человеческих возможностей // Мировая наука и образование в условиях современного общества: Сборник научных трудов по материалам Международной научно-практической конференции 30 октября 2014 г. – М.: АР-Консалт, 2014.
19. Стратегия национальной безопасности Российской Федерации до 2020 года [Электронный ресурс]. – URL: http://spbstrategy2030.ru/ ?page_id=102 (дата обращения 15.03.2015).
20. *Сен А.* Развитие как свобода / Пер. с англ. Е. Полецкой; Ред. и послесл. Р.М. Нуреева. – М.: Новое издательство, 2004. – 425 с.
21. *Буланов В.*, *Катайцева Е.* Человеческий капитал как форма проявления человеческого потенциала // Общество и экономика. – 2011. – № 1. – С. 13-22.
22. Официальный сайт Организации объединенных наций (ООН) [Электронный ресурс]. – URL: http://www.un.org/ru/index.html (дата обращения 23.03.2015).
23. *Ковылов В.К.* Современные научные возможности изучения человека и человеческого капитала // Географический вестник. – 2009. – № 1 [Электронный ресурс]. – URL: http://cyberleninka.ru/article/n/sovremennye-nauchnye-vozmozhnosti-izucheniya-cheloveka-i-chelovecheskogo-kapitala (дата обращения 27.02.2015).
24. *Бурцева И.В.*, *Любивая Ю.А.* Социальная работа в контексте проблемы развития человеческого потенциала // IX Студенческая международная заочная научно-практическая конференция «Научное сообщество студентов XXI столетия». Общественные науки. Россия, г. Новосибирск 21 марта 2013 г. [Электронный ресурс]. – URL: http://sibac.info/ studencheskie-konferentsii/nauchnoe-soobshchestvo-studentov-xxi-stoletiya-obshchestvennye-nauki/5783-5783 (дата обращения 27.02.2015).
25. *Черникова Д.В.*, *Черникова И.В.* Расширение человеческих возможностей: когнитивные технологии и их риски // Известия Томского политехнического университета. – 2012. – Т. 321. – № 6.
26. *Еникеева Л.А.*, *Карпова Г.В.* Моделирование износа человеческого капитала // Вестник ИНЖЭКОНа. – 2009. – Вып. 6(33). – С. 190.
27. Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года [Электронный ресурс]. – URL: http://www.ifap.ru/ofdocs/rus/rus006.pdf (дата обращения 15.05.2015).
28. *Гордеева Е.С.*, *Суслова С.В.* Измерение качества жизни: возможности муниципальной статистики // Вісник Київського національного університету ім. Тараса Шевченка. Серія: Економіка. – 2014. – № 157

[Электронный ресурс]. – URL: http://cyberleninka.ru/ (дата обращения 07.04.2015).

29. *Еникеева Л.А.*, *Ширшикова М.С.* Модель повышения конкурентоспособности экономики России на основе индикаторов качества жизни населения регионов // Стратегии и инструменты управления экономикой: отраслевой и региональный аспект: Сборник научных трудов по материалам V Международной научно-практической конференции 19-21 марта 2015 г. – СПб.: Университет ИТМО, 2015.

Научное издание

АКТУАЛЬНЫЕ ВОПРОСЫ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Под редакцией д-ра экон. наук, проф. Е. В. Стельмашонок

Подписано в печать 27.11.15. Формат 60×84 1/16.
Усл. печ. л. 10,25. Тираж 500 экз. Заказ 1658.

Издательство СПбГЭУ. 191023, Санкт-Петербург, Садовая ул., д. 21.

Отпечатано на полиграфической базе СПбГЭУ