Разработка комплексной системы защиты информации в ЛВС дорожно-строительной организации

En **Development Complex Information Security System in the LAN of Road-building Organizations**

E. K. Bragina,
Engineer
BraginaEK@gumrf.ru

V. D. Gaskarov,
Doctor of Engineering Sciences, Professor
GaskarovBD@gumrf.ru

S. S. Malov,
Senior Lecturer
MalovSS@gumrf.ru

Admiral Makarov State University of Maritime and Inland Shipping

V. G. Shved,
Doctor of Engineering Sciences
school@gkspr.ru
Training Center «SpecProject»

This article discusses the development of a complex information security system in the LAN of road-building organizations, aimed at preventing various types of impacts for the protected information. In the study was an analysis of the object of protection and the information processed in the organization, categorization produced information on trade secrets and personal information. As a result, current threats and the necessary level of security were identified. The above analysis, the requirements to a complex system of protection and the necessary methods and means of information protection were offered.

Keywords:information security, security of the local area network, personal data, trade secrets

В данной статье рассматривается вопрос разработки комплексной системы защиты информации в локальной вычислительной сети дорожно-строительной организации, направленной на предотвращение различного рода воздействий на защищаемую информацию. В процессе исследования был проведен анализ объекта защиты и информации, обрабатываемой в организации, произведено категорирование информации на коммерческую тайну и персональные данные. Выявлены источники информации: внутренние и внешние. В результате определены актуальные угрозы и необходимый уровень защищенности. В соответствии с нормативно-правовыми документами, а также исходя из проведенного анализа, сформулированы требования к комплексной системе защиты и предложены необходимые организационные, технические и программно-аппаратные методы и средства защиты информации.

Ключевые слова: информационные технологии, защита информации, система защиты информации, защита локальной вычислительной сети, персональные данные, коммерческая тайна, средства защиты информации

Елизавета Константиновна Брагина,
инженер
BraginaEK@gumrf.ru

Вагиз Диляурович Гаскаров,
доктор технических наук,
профессор кафедры КОИБ
GaskarovBD@gumrf.ru

Сергей Сергеевич Малов,
старший преподаватель кафедры КОИБ
MalovSS@gumrf.ru

ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова»

Виктор Григорьевич Швед,
доктор технических наук,
старший научный сотрудник
school@gkspr.ru

НОУ ДПО «Учебный центр «СпецПроект»

Введение

В современном мире для хранения, обработки и передачи различного рода информации широко используются информационные технологии (далее – ИТ). В связи с этим значительно возросло число информационных атак, приводящих к значительным финансовым и материальным потерям во всех направлениях деятельности человека, в том числе в результате утечек конфиденциальной информации.

Для организаций дорожно-строительной сферы конфиденциальную информацию могут составлять коммерческая тайна и персональные данные. От уровня защиты коммерческой тайны зависит развитие организации, спрос на предоставляемые услуги и увеличение прибыли. Персональные данные (далее – ПДн) сотрудников и клиентов организации также являются ценной информацией. Организация защиты ПДн регламентируется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и другими нормативно-правовыми актами. За не-

соблюдение требований данного закона предусмотрена административная, гражданско-правовая и уголовная ответственность [1].

Для разработки комплексной системы защиты информации (далее – ЗИ), обрабатываемой в локально вычислительной сети (далее – ЛВС) дорожно-строительной организации в соответствии с нормативно-правовыми требованиями законодательства Российской Федерации необходимо решить следующие задачи:

1) провести обследование объекта защиты;

2) провести анализ собранной информации;

3) на основе результатов анализа разработать комплексную систему защиты информации (далее – СЗИ) в ЛВС дорожно-строительной организации;

4) провести экономическое обоснование проекта;

5) выработать рекомендации по внедрению СЗИ;

6) рассмотреть дальнейшее развитие разработанной комплексной СЗИ.

Обследование объекта

Дорожно-строительная организация выполняет работы по ремонту и строительству дорог, оказывает комплексные услуги в сфере автодорожных работ, строительства инженерных сетей, спортсооружений, инженерной подготовки территорий, благоустройства и озеленения территорий. Организация имеет постоянно пополняемый парк специализированной дорожно-строительной техники, которая снабжена соответствующими сертификатами качества и регулярно проходит плановое техническое обслуживание. Все имеющиеся лицензии оформлены в соответствии с требованиями законодательства РФ. Организация обеспечивает высокое качество работ и их безопасность.

Дорожно-строительная организация арендует помещения на первом этаже двухэтажного здания, расположенного на огороженной забором территории. В данном здании размещаются административные отделы и ЛВС.

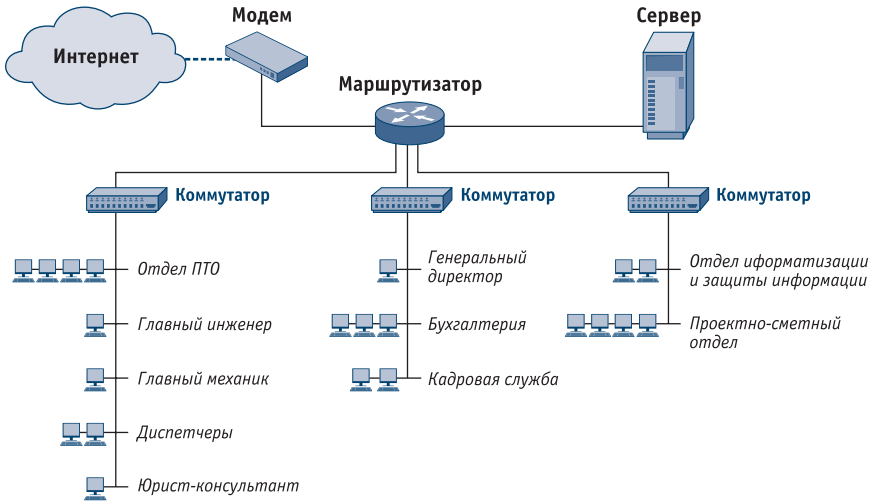

Рис. 1. ***Логическая схема ЛВС***

Главной целью организации является ее развитие, приводящее к получению высокой прибыли, которая основана на предоставлении услуг в сфере автодорожного строительства.

Задача дорожно-строительной организации – разработка мероприятий, обеспечивающих выполнение и сдачу установленных дорожно-строительных работ в проектные сроки, с высоким качеством и минимальными затратами.

В состав ЛВС дорожно-строительной организации входят следующие элементы: сервер, рабочие станции, периферийные устройства, сетевое оборудование.

Сервер, работающий под управлением ОС Windows Server 2008, выполняет ряд функций:

- контроллер домена, контролирующий область компьютерной сети и поддерживающий политику защиты;
- сервер базы данных (далее – БД), выполняющий обработку различных запросов, направленных БД;
- файл-сервер, предназначенный для хранения и обмена файлов любого типа;
- прокси-сервер, подключающий локальную сеть к сети Интернет.

Данная организация имеет 20 рабочих станций. Каждая оснащена операционной системой Windows 7 и имеет основной пакет прикладных программ, необходимых для решения профессиональных задач, свойственных деятельности работников организации. В состав специализированного программного обеспечения (далее – ПО) входит: MS Office, «1С: Зарплата и кадры», «1С: Кадры», AutoCAD, «КонсультантПлюс».

Периферийные устройства, входящие в состав локальной сети дорожно-строительной организации, представляют собой: факс (1 штука), принтер (4 штуки), МФУ (3 штуки).

Также при обследовании было выявлено наличие активного сетевого оборудования: коммутатор Tenda G1008D (2 штуки), коммутатор Tenda S16 (1 штука), модем D – Link (1 штука), маршрутизатор Mikrotik CCR1009-8G-1S-1S (1 штука).

Данная сеть обеспечивает обмен информацией в рамках организации и обеспечивает возможность взаимодействия с глобальной сетью Internet. На рис. 1 представлена логическая схема ЛВС организации.

В результате обследования объекта и определения логической схемы ЛВС построена структурная схема размещения основных технических средств и систем (далее – ОТСС) относительно границ контролируемой зоны (далее – КЗ) (рис. 2).

Анализ собранной информации

С помощью анализа информации, обрабатываемой в организации, было установлено, что конфиденциальная информация (или информация ограниченного доступа) в организации подразделяется на коммерческую тайну и персональные данные, которые, в свою очередь, от-

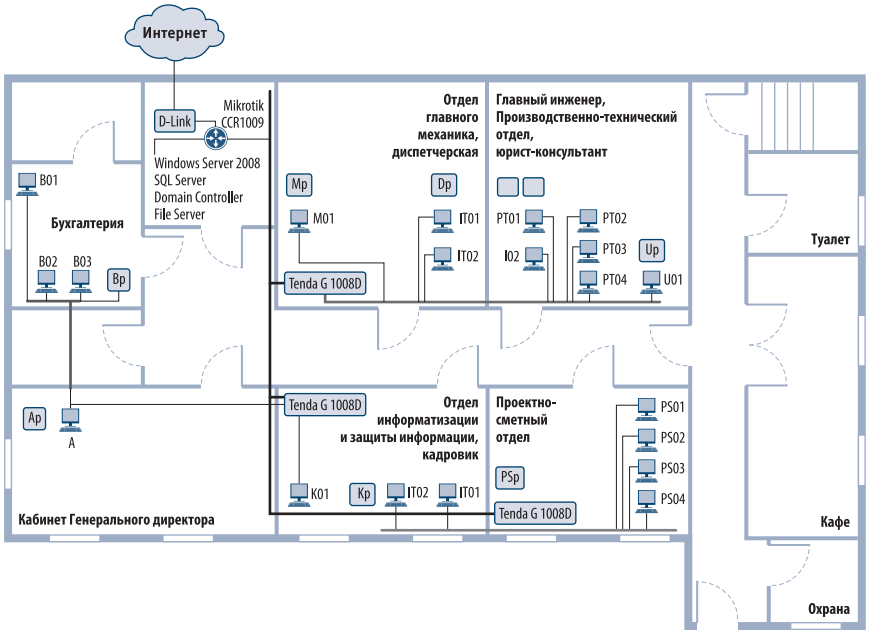

Рис. 2. ***Структурная схема ОТСС относительно границ КЗ***

носятся к ПДн сотрудников или ПДн клиентов. На объекте защиты отсутствуют сведения, составляющие государственную тайну.

Отнесение конкретных сведений к коммерческой тайне осуществляется руководителем дорожно-строительной организации. Перечень информации, составляющей коммерческую тайну данной организации, содержит следующие сведения:

- о состоянии программного и компьютерного обеспечения и пароли доступа;
- об особенностях используемых и разрабатываемых технологий и специфике их применения;
- о применяемых оригинальных методах управления, системах планирования и контроля;
- о подготовке, принятии и исполнении отдельных решений руководителем организации по производственным, коммерческим, организационным и другим управленческим вопросам;
- о системе поощрения и мотивации;
- о размере и составе имущества организации;
- бухгалтерской отчетности;
- о кругообороте средств и финансовых операциях организации;
- о долговых обязательствах и состоянии кредита организации;
- о размере прибыли организации;
- о бизнес-планах организации;
- о целях, рассматриваемых вопросах, результатах, фактах проведения совещаний и заседаний в организации, принятых решениях, сотрудниках, принимавших участие в их подготовке, и работе;
- о содержании различного рода договоров, заключенных организацией, и ходе их исполнения;
- о подготовке к участию в конкурсах, аукционах, тендерах и их результатах;
- о порядке и состоянии организации защиты коммерческой тайны;
- о порядке и состоянии организации охраны, пропускном режиме, системе сигнализации.

В данной организации БД состоят из сведений, составляющих ПДн, под которыми понимается любая информация, относящаяся к определенному физическому лицу [2]. В своей работе БД сотрудников и клиентов используют генеральный директор, бухгалтерия и отдел кадров. Генеральный директор имеет доступ ко всем сведениям.

В бухгалтерии обрабатываются следующие сведения, относящиеся к ПДн сотрудников:

- фамилия, имя, отчество (в том числе предыдущие);
- серия и номер паспорта, кем и когда выдан;
- информация о гражданстве;
- дата и место рождения;
- адрес прописки и проживания;
- телефонные номера (домашний и мобильный);
- состояние в браке и состав семьи;
- ИНН и СНИЛС;
- справка 2-НДФЛ с предыдущего места работы;
- должность;
- период работы и данные о трудовом договоре;
- сведения о доходах и заработной плате;
- исполнительные листы;
- лицевые счета;
- сведения о квалификации и переподготовке;
- иные ПДн, необходимые для бухгалтерской деятельности.

Сведения, составляющие ПДн сотрудников, обрабатываемые в системе отдела кадров:

- фамилия, имя, отчество, дата и место рождения;
- паспортные данные и гражданство;
- адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
- номера телефонов (мобильного и домашнего);
- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки;
- сведения о повышении квалификации и переподготовке;
- сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
- сведения о трудовой деятельности;
- сведения о воинском учете военнообязанных лиц и лиц, которые подлежат призыву на военную службу;
- сведения о страховом свидетельстве государственного пенсионного страхования;
- сведения о семейном положении;
- сведения из страховых полисов обязательного медицинского страхования;
- сведения об идентификационном номере налогоплательщика;
- сведения из заключения по результатам прохождения медицинского осмотра;
- сведения о временной нетрудоспособности;
- сведения о водительском удостоверении;

- анкетные и биографические сведения.

ПДн уволенных сотрудников хранятся в БД организации на протяжении 5 лет, по истечении срока хранения – уничтожаются.

Также в БД организации хранятся ПДн клиентов:

- физических лиц, обратившихся в организацию с целью получения предоставляемых услуг;
- индивидуальных предпринимателей и физических лиц – представителей юридических лиц, фигурирующих в договорах, контрактах.

Сведения, составляющие ПДн клиентов дорожно-строительной организации, представлены в табл. 1.

Таблица 1. ***Персональные данные (далее – ПДн) клиентов***

Сведения, составляющие персональные данные	Физические лица	Индивидуальные предприниматели и представители юридических лиц
Фамилия, имя, отчество	+	+
Паспортные данные	+	+
Адрес электронной почты	+	+
Контактный телефон	+	+
Юридический адрес		+
ИНН, КПП, р/с, БИК		+

В организации существуют внутренние (обмен данными между сотрудниками организации) и внешние (потоки получения информации из внешней среды организации) информационные потоки. Из внешней среды организация взаимодействует с: поставщиками, лизинговыми компаниями, конкурентами, государственными органами, клиентами, банками, налоговой инспекцией, пенсионным фондом и негосударственными организациями.

При разработке комплексной системы защиты стоит учесть тот факт, что автоматизированные рабочие места (далее – АРМ), работающие с ПДн, физически неразрывны, так как связанны одним коммутатором и имеют выход в Интернет. Также существует необходимость предоставления этих ПДн определенным представителям из внешней среды.

Разработка комплексной системы защиты информации в ЛВС дорожно-строительной организации

Целесообразно будет разделить информационную систему (далее – ИС) организации на сегменты, то есть с помощью дополнительного коммутатора физически разделить среды обработки ПДн и коммерческой тайны. Это позволит определить набор требований, мер и защитных средств для каждого сегмента сети, что обеспечит адекватную защиту по каждому из них и в целом всей ИС.

Для организации комплексной защиты конфиденциальной информации необходимо проанализировать нормативно-правовую базу по защите ПДн и коммерческой тайны. Необходимо учесть, что АРМы, обрабатывающие и не обрабатывающие ПДн, соединены одним коммутатором, что может нести в себе дополнительные угрозы.

Построение защищенной ИС ПДн

Нормативная база защиты ИС для дорожно-строительной организации состоит из Конституции РФ, Трудового кодекса РФ от 30.12.2001 г. № 197-ФЗ и соответствующих руководящих документов [2–9].

ИС дорожно-строительной организации обрабатывает ПДн сотрудников и клиентов в количестве менее 100 000 субъектов. Организация подвержена угрозам 2-го типа: наличие недокументированных возможностей в прикладном ПО, используемом в ИС. Следовательно, организация нуждается в обеспечении 3-го уровня защищенности ПДн и сотрудников, и клиентов.

Требования к системе ЗИ определяются в зависимости от класса защищенности ИС и угроз безопасности информации [10]. Для обеспечения надежной защиты ИС ПДн организации необходимо соответствовать требованиям, предъявляемым к обеспечению 3-го уровня защищенности ПДн.

В состав мер по обеспечению безопасности ПДн организации, реализуемых в рамках системы защиты ПДн с учетом 2-го типа актуальных угроз безопасности ПДн и применяемых ИТ, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн);
- регистрация событий безопасности;
- антивирусная защита;
- контроль (анализ) защищенности ПДн;
- защита технических средств;
- защита ИС, ее средств, систем связи и передачи данных;
- управление конфигурацией ИС и системы защиты ПДн.

При использовании в ИС сертифицированных по требованиям безопасности информации, средств ЗИ для обеспечения 3-го уровня защищенности ПДн, должны применятся [4]:

- средства вычислительной техники не ниже 5-го класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4-го класса защиты в случае актуальности угроз 2-го типа или взаимодействия ИС с информационно-телекоммуникационными сетями международного информационного обмена;
- межсетевые экраны не ниже 3-го класса в случае актуальности угроз 2-го типа или взаимодействия ИС с информационно-телекоммуни-

Таблица 2. ***Сертифицированные технические средства ЗИ***

Тип СЗИ	Средство защиты информации	Условное обозначение и номер меры
Средство защиты информации от НСД	Dallas Lock 8.0 – С	• ИАФ.1, ИАФ.2, ИАФ.4; • РСБ.1 – РСБ.4; • УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.7, УПД.8; • ЗНИ.1
Средство защиты информации	Security Studio Endpoint Protection	• АВ3.1, АВ3.2; • СОВ1, СОВ2
Сканер безопасности	RedCheck	• АН3.1 – АН3.4; • УКФ.2, УКФ.4
Межсетевой экран	Cisco ASA – 5510	• УПД.3; • ЗИС.1

кационными сетями международного информационного обмена и межсетевые экраны не ниже 4-го класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия ИС с информационно-телекоммуникационными сетями международного информационного обмена.

Для обеспечения 1-го и 2-го уровней защищенности ПДн, а также для обеспечения 3-го уровня защищенности ПДн в ИС, для которых к актуальным отнесены угрозы 2-го типа, применяются средства ЗИ, ПО которых прошло проверку не ниже чем по 4-му уровню контроля отсутствия недекларированных возможностей [4].

Выбор сертифицированного средства защиты ИСПДн может осуществляться только после анализа государственного реестра сертифицированных средств ЗИ. На основании анализа данного реестра и соответствующего приказа для реализации необходимых мер и для надежного обеспечения защиты ПДн дорожно-строительной организации предлагается набор сертифицированных технических средств ЗИ, представленный в табл. 2.

Помимо вышеперечисленных средств защиты на сервер необходимо установить защищенный программный комплекс «1С: Предприятие 8.2».

Меры ИАФ.3, ЗТС.1, ЗТС.2, УКФ.1, УКФ.2 реализуются с использованием организационных мероприятий, применение которых подразумевает разработку комплекта документов и проведение работ с персоналом.

Построение системы защиты коммерческой тайны

С самого начала следует грамотно определить правовой статус конфиденциальной информации, а также необходимые требования и меры для обеспечения ее защиты. Кроме того, необходимо не забывать сопоставлять интересы организации с интересами государства.

Необходимо определить сведения, составляющие коммерческую тайну и распределить их по категориям важности, учитывая их ценность и важность для организации, а так же определить негативные последствия, которые могут возникнуть при разглашении этих сведений. Также следует учесть, что если переусердствовать с мерами защиты доступа к информации, то появляется риск осложнения работы организации, что приведет к экономическим растратам.

Сведения, составляющие коммерческую тайну дорожно-строительной организации и нуждающиеся в защите, удовлетворяют следующим критериям [11]:

1) их открытое использование наносит ущерб организации;

2) они не являются общедоступными и общеизвестными на законных основаниях;

3) организация должна предпринимать необходимые меры, не нарушающие их конфиденциальность, для финансовой и другой выгоды;

4) им необходима защита, так как они не являются государственной тайной и не защищены авторским или патентным правом;

5) их сокрытие не противоречит интересам государства и общества.

В ходе анализа нормативно-правовых документов авторами были сформированы актуальные требования для построения надежной защиты коммерческой тайны организации [5, 6, 12]:

- идентификация, проверка подлинности и контроль доступа субъектов;
- управление потоками информации;
- регистрация и учет;
- учет носителей информации;
- очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей;
- обеспечение целостности программных средств и обрабатываемой информации;
- физическая охрана средств вычислительной техники и носителей информации;
- периодическое тестирование СЗИ НСД;
- наличие средств восстановления СЗИ НСД;
- защита от вредоносных программ;
- наличие МЭ, при существовании возможности подключении ЛВС организации к сети Интернет.

Меры по охране конфиденциальности информации признаются разумно достаточными, если исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя и обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны [9].

Таким образом, в качестве основных мер в этом направлении будем принимать следующие:

- документальное оформление перечня сведений, составляющих коммерческую тайну дорожно-строительной организации;
- ограничение доступа персонала и посторонних лиц в защищаемые помещения;

- учет лиц, получивших доступ к коммерческой тайне, а также лиц, которым она была передана;
- разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей ИС, контроль за несанкционированным доступом и действиями пользователей;
- учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение;
- необходимое резервирование технических средств и дублирование массивов и носителей информации;
- оптимальное ограничение числа лиц, имеющих допуск к информации, составляющей коммерческую тайну;
- использование защищенных каналов связи;
- размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр информации;
- предотвращение внедрения в автоматизированные системы программ-вирусов, программных закладок.

В табл. 3 представлен выбор решений для реализации вышеперечисленных требований.

Организация работ по созданию и эксплуатации объектов информатизации и их СЗИ определяется в разрабатываемом в организации «Руководстве по защите коммерческой тайны». Она должна предусматривать [6]:

1) порядок определения защищаемой информации;

2) порядок привлечения подразделений организации, специализированных сторонних организаций к разработке и эксплуатации объектов информатизации и СЗИ, их задачи и функции на различных стадиях создания и эксплуатации объекта информатизации;

3) порядок взаимодействия всех занятых в этой работе организаций, подразделений и специалистов;

Таблица 3. ***Выполнение требований по защите коммерческой тайны***

Направление защиты	Решение	Выполняющиеся требования
Техническое	Использование встроенных механизмов операционной системы Windows 7, групповые политики	• Идентификация, проверка подлинности и контроль доступа субъектов; • регистрация и учет; • очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей; • обеспечение целостности программных средств и обрабатываемой информации; • периодическое тестирование СЗИ НСД; • наличие средств восстановления СЗИ НСД
	Межсетевой экран Cisco ASA	• Управление потоками информации; • наличие МЭ, при существовании возможности подключении ЛВС организации к сети Интернет
	Средство антивирусной защиты Kaspersky Security	Защита от вредоносных программ
	Программный комплекс DeviceLock	Ограничения доступа к съемным носителям, контроль печати
Правовое	Создание соответствующих документов	Учет носителей информации; физическая охрана средств вычислительной техники и носителей информации

4) порядок разработки, ввода в действие и эксплуатацию объектов информатизации;

5) ответственность должностных лиц за своевременность и качество формирования требований по технической защите информации, за качество и научно-технический уровень разработки СЗИ.

Комплексная система защиты информации

Для реализации комплексной СЗИ в ЛВС дорожно-строительной организации следует:

- проводить организационные мероприятия с персоналом по ЗИ;
- разработать дополнительную документацию;
- приобрести и установить выбранные программные и аппаратные средства защиты;
- приобрести и подключить дополнительный коммуникатор для работы с ПДн клиентов;
- приобрести телекоммуникационные настенные шкафы с замком.

На рис. 3 представлена логическая схема ЛВС дорожно-строительной организации с применением выбранных конкретных защитных средств для обеспечения безопасности ПДн и коммерческой тайны.

Стадия ввода в эксплуатацию комплексной системы защиты информации

Финальным этапом создания защищенной ИС должна стать аттестация или декларирование соответствия.

Под аттестацией понимается комплекс проводимых мероприятий, которые подтверждают соответствие ИС требованиям по безопасности информации согласно нормативно-методическим документам ФСТЭК России. Документ подтверждения называется «Аттестат соответствия» и дает право на обработку информации соответствующего уровня конфиденциальности в течение трех лет [13].

Важным моментом является то, что в случае каких-либо изменений обработки ПДн требуется проведение дополнительной проверки эффективности системы защиты ИС ПДн.

Обязательной аттестации подлежат информационные системы, обрабатывающие сведения, составляющие государственную тайну, а также и обеспечивающие ведение секретных переговоров и управление экологически опасными объектами. В остальных случаях аттестация носит добровольный характер и может

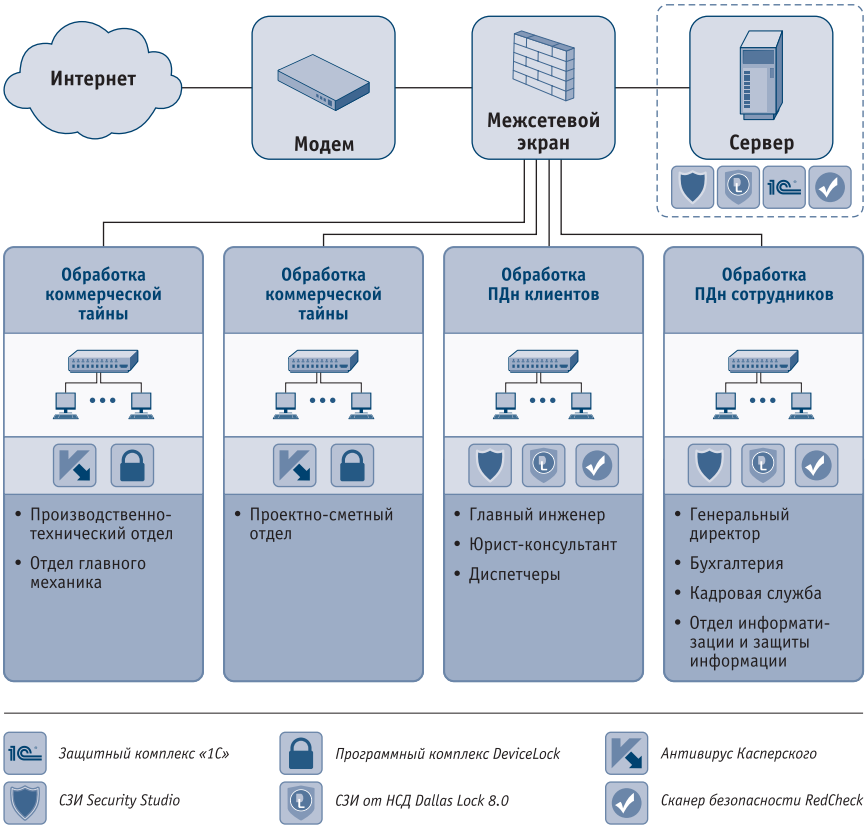

Рис. 3. ***Логическая схема ЛВС после применения СЗИ***

осуществляться по желанию заказчика.

Для ИСПДн не определена обязательная форма оценки соответствия, следовательно, можно определить форму и содержание оценки соответствия самостоятельно [12]. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже одного раза в 3 года в сроки, определяемые оператором (уполномоченным лицом) [5]. Для утверждения проведенной работы оператор оформляет декларацию соответствия. На сегодняшний момент процедура декларирования не регламентирована для коммерческих организаций, то есть, как и процедура аттестации, является добровольной. Оператор, при наличии квалификации и необходимых сертифицированных средств, может проводить декларирование соответствия ИСПДн требованиям защиты и оформление «Декларации соответствия» самостоятельно, в отличие от аттестации, которую проводят только организации, имеющие лицензию ФСТЭК России на данный вид деятельности [14–19].

Экономическое обоснование

Экономическое обоснование является оценкой совокупности стоимости внедрения разработанного проекта. Оно доказывает, что использование выбранного необходимого оборудования, программных средств и мер будет рентабельным. Стоимость проекта включает в себя стоимость закупленного оборудования, аппаратных и программных средств, а также затраты на обновление последних.

На сегодняшний день искажение, утечка, утрата, несанкционированный доступ к информации, обрабатываемой в ЛВС дорожно-строительной организации, способны нанести ущерб гораздо больший, чем средства, потраченные на внедрение комплексной СЗИ ЛВС.

Дальнейшее развитие комплексной системы защиты информации

В случае значительного расширении штата дорожно-строительной организации, с учетом потенциального увеличения объемов обрабатываемой информации, необходимо развивать ЛВС в территориально распределенную информационную сеть и, как следствие, провести работы по модернизации комплексной СЗИ. В частности, к таким работам можно отнести:

- сертификацию информационной системы в соответствии с международными стандартами;
- проведение аттестации ИСПДн;
- построение системы комплексного мониторинга действий пользователей в ИС, включая внедрение системы IP-видеонаблюдения.

Заключение

В результате проведенного анализа было принято решение, что ИС организации необходимо разделить на сегменты, а именно, на сегменты, обрабатывающие коммерческую тайну, сегмент обработки ПДн клиентов и сегмент обработки ПДн сотрудников. Такое решение позволило рассмотреть каждый сегмент в отдельности и разработать эффективную комплексную защиту всей информации.

Кроме разработки комплексной системы защиты информации в данной статье предложены рекомендации по вводу в эксплуатацию, а также рассмотрен вариант дальнейшего развития проекта.

С целью совершенствования системы защиты рекомендуется:

- осуществлять более тщательный контроль соблюдения правил работы сотрудников организации с ПДн и конфиденциальной информацией;
- проводить регулярные проверки и обслуживать все ИС и информационные инфраструктуры на работоспособность;
- снабдить ключевые элементы информационно-вычислительной сети организации источниками бесперебойного питания. ■

ЛИТЕРАТУРА

1. Омаров В. К. Ответственность за нарушение требований по защите персональных данных // Information Security/Информационная безопасность. – 2011. – № 3. – С. 37.

2. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.12.2013) «О персональных данных».

3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5. Руководящий документ от 30.03.1992 «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем».

6. Руководящий документ 30.08.2002 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К).

7. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».

8. Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

9. Федеральный закон Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

10. Капустина А. Защита государственных информационных систем выходит на новый уровень // Защита информации. Инсайд. – 2013. – № 6. – С. 46–49.

11. Муравьев А. И., Игнатьев А. М., Крутик А. Б. Предпринимательство: Учебник. – СПб: Изд-во «Лань», 2001. – 235 с.

12. Руководящий документ ФСТЭК России от 25.12.2006 «Методические рекомендации по технической защите информации, составляющей коммерческую тайну».

13. Электронные лекции [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/studies/courses/2291/591/lecture/12685/.

14. Соколов С. С., Малов С. С., Карпина А. С. Построение защищенной информационной системы персональных данных мониторингового центра оказания телематических услуг безопасности на транспорте // Вестник ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова». – 2014. – № 5. – С. 148–157.

15. Соколов С. С. Модель угроз информационной безопасности организации // Журнал Университета водных коммуникаций. – СПб.: СПГУВК, 2009 (Вып.2). – с. 176–180.

16. Нырков А. П., Соколов С. С., Вайгандт Н. Ю. Обеспечение безопасности автоматизированных систем управления движением судов при помощи технологии референцных станций // Морская радиоэлектроника. – 2013. – № 2 (44). – С. 48–50.

17. Нырков А. П., Рудакова С. А. Методика аудита объектов информатизации по требованиям информационной безопасности // Журнал Университета водных коммуникаций. – 2012. – № 3. – С. 146–149.

18. Консультант плюс – надежная правовая поддержка [Электронный ресурс]: Режим доступа: http://www.consultant.ru/.

19. Официальный сайт ФСТЭК России [Электронный ресурс]: Режим доступа: http://fstec.ru/.

НОВОСТИ

Новые сервисы и интегрированные облачные решения Cisco

Cisco представила ряд новых сервисов и облачных ИБ-решений, в основе которых лежит ориентированная на угрозы архитектура безопасности Cisco. В сети, в оконечных точках и в облаке архитектурный подход Cisco позволяет выявить больше угроз, помогая заказчикам сократить время обнаружения в среднем до 17 часов (стандартный отраслевой показатель составляет 100 дней).

Объединяя беспрецедентную обозреваемость сети с разнообразием интегрированных продуктов, Cisco упрощает распределенным и мобильным предприятиям задачу эффективного обеспечения безопасности там, где это необходимо – в филиале, в главном офисе, у конечного пользователя, где бы он ни находился. Cisco встраивает средства обеспечения информационной безопасности в проходимые пользователем точки подключения, поэтому сеть, точки доступа и оконечные точки находятся в безопасности уже до того, как пользователь зарегистрируется в сети.

Cisco разработала ряд решений и сервисов, упрощающих заказчикам защиту их информационных ресурсов.

- *Cisco Umbrella Roaming.* Централизованное облачное решение, устраняющее «слепые пятна» вне сети и защищающее сотрудников в роуминге, где бы они ни находились.
- *Cisco Umbrella Branch.* Облачное решение, позволяющее предприятию контролировать гостевое использование сети Wi-Fi с помощью простой контент-фильтрации.
- *Cisco Defense Orchestrator.* Облачное решение с консольным интерфейсом для простого и эффективного управления крупными инфраструктурами и политиками информационной безопасности в распределенных конфигурациях с тысячами устройств.
- *Cisco Meraki MX.* Полностью облачно управляемое унифицированное решение управления угрозами (UTM) обеспечивает защиту филиалов от вредоносного ПО путем проверки файлов по облачной базе данных для выявления вредоносного контента и блокирования файлов до их загрузки пользователями.
- *Cisco Stealthwatch Learning Network License.* Этот компонент позволяет маршрутизаторам Cisco ISR играть роль устройства обнаружения и исполнителя политик безопасности для филиалов.