МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Политехнический институт: Заочный
Кафедра «Системы автоматического управления»

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой

_____/ В.И. Ширяев

«_____» _____ 2018 г.

МОДЕРНИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СЕТЕВОЙ ИНФРАСТРУКТУРЫ АДМИНИСТРАЦИИ ГОРОДА

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 09.03.01.2018.075.00 ПЗ ВКР

Руководитель работы
нач. отд. защиты информации
администрации г. Н. Уренгой

_____/ Е.Р. Ахметзянов

«____» _____ 2018 г.

Автор работы
студент группы ПЗ-597

_____/ П.М. Марков

«____» _____ 2018 г.

Нормоконтролер
ст. преп. каф. САУ

_____/ В.П. Щербаков

«____» _____ 2018 г.

Челябинск 2018

АННОТАЦИЯ

Марков П.М. Модернизация системы информационной безопасности и сетевой инфраструктуры администрации города: ЮУрГУ (НИУ), ПИ: Заочный; 2018, 80 с. 14 ил., библиогр. список – 32 наим., 14 листов слайдов презентации ф. А4.

Для разработки комплекса мер по повышению уровня информационной безопасности администрации города Новый Уренгой проведен анализ информационной безопасности администрации города Новый Уренгой, составлена методология оценки информационной безопасности по опросным листам, проведены реорганизационные работы по повышению уровня информационной защищенности.

В результате выполнения работы разработаны организационные и технические меры повышения информационной безопасности в администрации города. Принятие данных мер позволяет повысить уровень информационной защищенности и привести его к современным требованиям.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Администрация города Новый Уренгой является исполнительно-распорядительным органом муниципального образования, наделенным полномочиями по решению вопросов местного значения и полномочиями для осуществления отдельных государственных полномочий. В ходе своей деятельности администрация ведет интенсивный обмен электронного документооборота, что накладывает жесткие требования к персональным данным и защите информации в целом [3].

Целью выпускной квалифицированной работы является создание комплекса мер по модернизации и обеспечению безопасности администрации города Новый Уренгой (далее - Администрация). Данные меры необходимы и создаются именно для того, чтобы справиться с проблемами информационной защищенности, не снижая уровня автоматизации и производственной деятельности при повседневных операциях. Особое внимание планируется уделить мерам предоставления сотрудникам и пользователям необходимой информации, сохраняя целостность данных и сети [3]. В работе планируется:

– проанализировать предприятие и применяемые информационные технологии на нем;

– охарактеризовать применяемые информационные технологии и системы защиты действующие в настоящее время;

– определить стратегии и планирование работ по развитию информационной структуры предприятия;

– рассмотреть организационное обеспечание информационной системы предприятия, оценку эффективности применяемых информационных систем и технологий.

На основе проделанной аналитической работы необходимо разработать комплекс организационно-правовых и технических мер защиты информационной среды администрации города Новый Уренгой. В виду большого количества специальных терминов и определений в ВКР планируется также привести сводную ведомость по всему используемому понятийному аппарату.

В настоящее время в департаменте ИТ города Новый Уренгой вопросам информационной безопасности уделяется недостаточное внимание, что отрицательно отражается на операционной деятельности и ведения муниципальной деятельности. В результате проведения комплекса мер, планируемых в проекте, ожидается вывод безопасности информационной системы на качественно новый уровень управляемости и масштабируемости, а также функционала для новых проектов и задач.

1 АУДИТ ИНФРАСТРУКТУРЫ АДМИНИСТРАЦИИ

1.1 Постановка задачи

В данной главе планируется произвести аудит инфроструктуры администрации, характеристику объекта проектирования, анализ информационной инфраструктуры администрации, анализ сетевой инфраструктуры администрации, целеполагание проекта информационной безопасности.

1.2 Характеристика объекта проектирования

Новый Уренгой - город окружного значения и муниципальное образование, городского округа в составе Ямало-Ненецкого автономного округа России. Административный центр - город Новый Уренгой [3].

Специализация муниципальной организации:

– муниципальная бюджетная организация;

– ведение социально-экономической политики города.

С точки зрения обеспечения безопасности, здание обеспечено системами видеонаблюдения. Безопасность объекта обеспечивается сотрудниками вневедомственной охраны и введенным пропускным режимом.

Физическую охрану осуществляет частное охранное предприятие ООО ЧОП «Северный оплот», обеспечивающее пропускной контроль и правопорядок на всех объектах муниципальной организации. Частное охранное предприятие выполняет функции согласно заключенному контракту, заключенному через площадку Госторги в 2015 году.

1.3 Анализ информационной инфраструктуры администрации

Современное предприятие невозможно представить без средств автоматизации информатизации и электронного обмена. В администрации города Новый Уренгой инфообмен ведется на целом парке персональных компьютеров с использованием ниже приведенного комплекса программного обеспечения [3]. Информационные системы, относящиеся, к ИСПДн:

– 1С: Предприятие 8.3 – Бухгалтерия;

– 1С: Бюджет;

– 1С: Зарплата;

– система CRM;

– система учета рабочего времени;

– Windows 10 на рабочих ПК;

– антивирус KIS 2017 в серверном и клиентском исполнении.

Предварительный анализ информационной инфраструктуры администрации города Новый Уренгой показал, что на рабочих ПК и сервере установлено антивирусное ПО, однако на всех терминалах присутствует открытый доступ к сети Интернет. Также стоит сказать, что на компьютерах сотрудников администрации установлено достаточно много нерегламентированного, свободного, бесплатного и пиратского софта, который сам может нести потенциальную угрозу.

К специализированным программным комплексам, непосредственно влияющих на деятельность управления администрации города Новый Уренгой являются:

– программный комплекс «Муниципальное самоуправление-СМАРТ»;

– программный комплекс «Реестр государственных услуг».

1). Автоматизация местного самоуправления для администрации муниципальных районов, городских округов, городских и сельских поселений («Муниципальное самоуправление - СМАРТ») [4].

Программный комплекс «Муниципальное самоуправление-СМАРТ» («МСУ-СМАРТ») - решение для комплексной автоматизации деятельности органов местного самоуправления и актуализации располагаемой ими информации для управления социально-экономическими показателями муниципальных образований и региона в целом.

Суть решения заключается в создании единой централизованной информационной системы муниципальных образований на уровне региона (муниципального района), интегрирующей в себе информационное хранилище, а также эффективные инструменты работы с ним на базе передовых Интернет-технологий.

Решаемые задачи МСУ-СМАРТ [4]:

– построение единой информационной системы муниципальных образований, содержащей информацию о населении, земле, имуществе, личных подсобных хозяйствах всех поселений региона;

– организация целенаправленной работы по повышению налогооблагаемой базы и привлечению дополнительных доходов в местные бюджеты;

– оказание государственных (муниципальных) услуг по запросам граждан в электронном виде (выдача регламентированных справок и выписок на основании записей похозяйственных книг);

– интеграция муниципальной информационной системы с информационными системами органов государственной власти;

– автоматизация делегированных муниципальным образованиям полномочий (первичный воинский учет и паспортно-визовая служба);

– предоставление руководству региона, администрациям муниципальных районов доступа к аналитической информации социально-демографического, финансово-экономического, налогового и статистического характера необходимой для принятия правильных управленческих решений;

выработка единого нормативно-справочного и методического пространства муниципальных образований [4].

2). Программный комплекс «Реестр государственных услуг» [5]

Типовой реестр государственных и муниципальных услуг применяется в органах государственной власти субъектов Российской федерации и муниципальных образованиях как Подсистема учета (формализации и хранения) и публикации информации о предоставлении государственных и муниципальных услуг органами власти. При этом объектами автоматизации являются государственные учреждения, являющиеся соучастниками программ и проектов ФЦП «Электронная Россия (2010-2020 годы)».

Основными возможностями являются:

– сбор и хранение информации о государственных и муниципальных услугах, оказываемых органами власти;

– сбор и хранение информации об органах власти, ответственных за предоставление государственных и муниципальных услуг;

– редактирование данных об услугах в государственных органах власти и муниципалитетах [5].

Основным предметом автоматизации являются функции в части сбора, хранения и редактирования информации о государственных и муниципальных услугах, а также информации об органах государственной власти, предоставляющих услуги.

С точки зрения безопасности и защиты персональных и конфиденциальных данных, выше приведенные специализированные программные комплексы наиболее подвержены уязвимостям и требуют особенного подхода к защите данных.

В муниципальных программных комплексах выполняется широкий круг задач, различными муниципальными служащими зачастую без допуска к секретным сведениям. Действительно, базы данных не представляют секретную информацию или сведения, содержащие гостайну, однако потеря, искажение, или кража информации ведет к существенным организационным, репутационным, финансовым и прочим рискам.

В виду большого количества сетевого обмена в специализированных программных комплексах «МСУ-СМАРТ» и «Реестр государственных услуг» необходимо регистрировать и отслеживать вносимые изменения в базу данных и проводимые сеансы с рабочих компьютеров администрации города Новый Уренгой. Защищать необходимо персональные данные и принятую нормативно-справочную информацию, и законодательные акты.

1.4 Анализ сетевой инфраструктуры администрации

В настоящее время в структуре информационной сетевой системы администрации города Новый Уренгой входит:

– пограничный маршрутизатор Cisco 2911R с коммутатором агрегации;

– 4 этажных коммутатора доступа Cisco 2960, 48 портов;

– 2 стоечных сервера HP Proliant DL (основной и резерв), выполняющие следующие виртуальные роли:

– СУБД;

– сервер почты IMAP;

– DHCP;

– сервер лицензий KIS 2017;

– персональные компьютеры и рабочие станции сотрудников администрации.

Ниже более подробно приведена характеристика используемого оборудования.

Маршрутизатор Cisco 2911 реализован для поддержки виртуальных соединений GETVPN, Enhanced Easy VPN, DMVPN. Максимальное количество подключений расширено до 150 человек. Два 10/100/1000 Мбит/с интерфейса предоставляют возможность высокоскоростной передачи [6].

Cisco 2911 интегрирует в себе все необходимые для офиса сервисы:

– маршрутизатора доступа и маршрутизатора локальной сети;

– центра IP-телефонии и голосовой почты;

– интегрированного решения для обеспечения безопасности;

– межсетевой экран;

– система предотвращения вторжений;

– шифрование и создание VPN-туннелей.

Для организации ЛВС администрации города и коммутации ПК сотрудников, задействованы стоечные коммутаторы доступа Cisco 2960/48, емкостью коммутатора 48 портов.

Семейство коммутаторов Cisco Catalyst 2960 представляет собой линейку коммутаторов с фиксированной конфигурацией с портами 10/100 или 10/100/1000 Мбит/с, предназначенных для офисов и филиалов.

Основные преимущества Cisco Catalyst 2960:

– интегрированная безопасность, включая поддержку NAC;

– улучшенная поддержка качества сервиса (QoS) и отказоустойчивости;

– одинаковый IOS Feature-Set для всех моделей;

– асинхронные потоки данных легко управляются;

– порты двойного назначения, позволяющие использовать подключение по медной паре или оптоволокну;

– сетевое управление, оптимизация пропускной способности;

– сетевая безопасность с использованием широкого диапазона методов идентификации, технологий кодирования данных, и сетевое управление по пользователю, порту и MAC адресу;

– ACL по портам для интерфейсов Layer2, фильтрация по MAC-адресам;

– динамическое назначение VLAN-ов.

В администрации города Новый Уренгой задействовано четыре коммутатора Cisco Catalyst 2960, емкостью 48 портов.

В качестве «ядра» вычислений и хранения БД использован новейший сервер HP Proliant DL [7]. Серверы нового поколения разработаны на основе сбалансированной архитектуры с применением новейших серверных технологий.

Пул IP адресации: 167.117.12.0/24 – внутренняя подсеть с обеспечение доступа через VPN. Информационная инфраструктура построена по централизованному принципу. Центральный департамент расположен в здании управления администрации города Салехард, в состав которой входят все муниципальные учреждения региона.

Сетевая инфраструктура построена по сетям VPN через арендованные каналы оператора ПАО «Ростелеком». За безопасность сетевой инфраструктуры отвечает сервер DMZ, который оперирует связью госсектора с внешней сетью Интернет [8]. Существующая сеть связи администрации города Новый Уренгой представлена на рисунке 1.1.

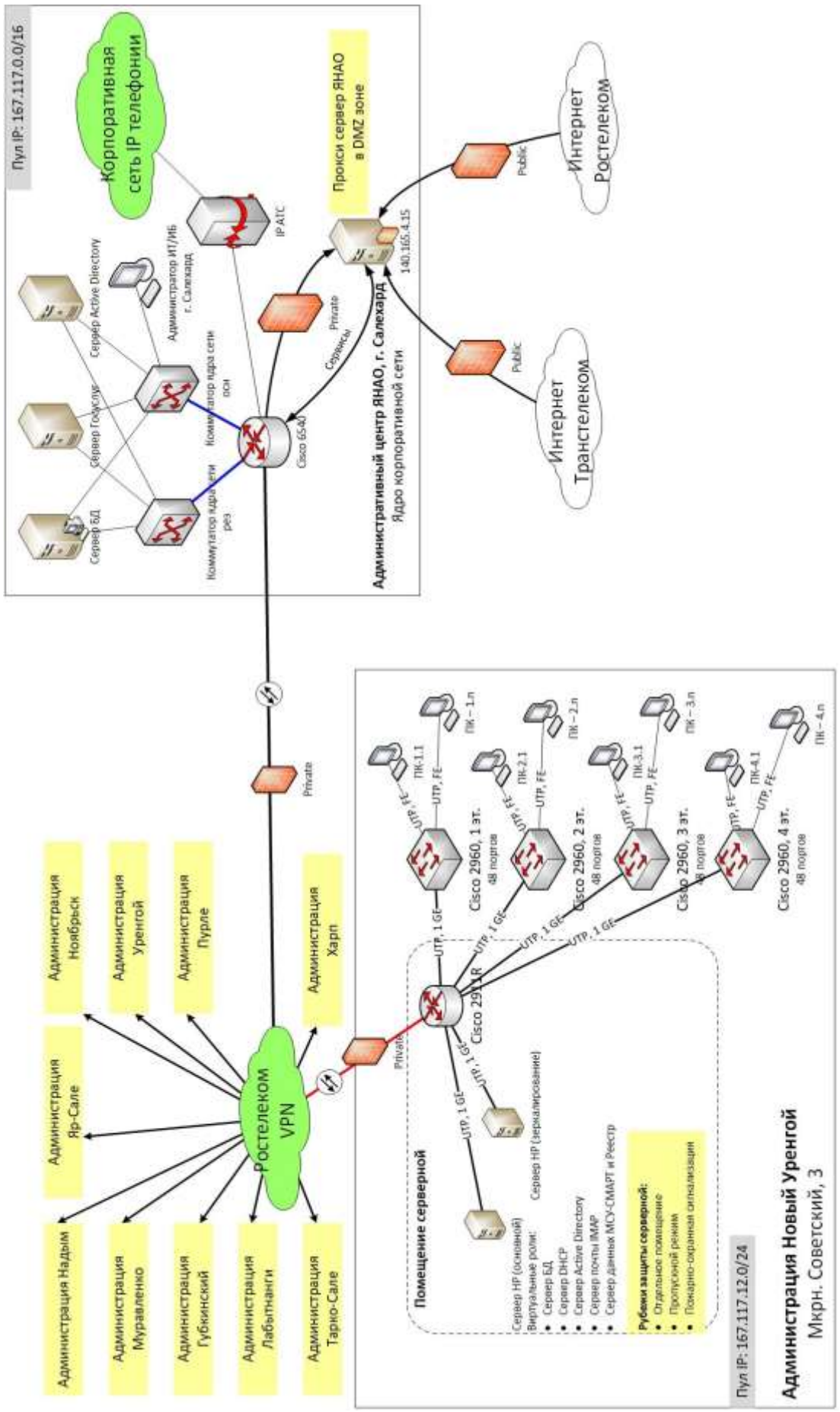
Пул IP: 167.117.0.0/16
Корпоративная сеть IP телефонии
IP АТС
Прокси сервер ЯНАО в DMZ зоне
Интернет Ростелеком
Public
Интернет Трансгелеком
Public
140.165.4.15
Сервер Active Directory
Администратор ИТ/ИБ г. Салехард
Сервер Госуслуг
Сервер БД
Коммутатор ядра сети ocs
Коммутатор ядра сети рез
Cisco 6540
Private
Сервисы
Административный центр ЯНАО, г. Салехард
Ядро корпоративной сети
Private
Ростелеком VPN
Администрация Ноябрьск
Администрация Уренгой
Администрация Пурпе
Администрация Харп
Администрация Яр-Сале
Администрация Надым
Администрация Муравленко
Администрация Губкинский
Администрация Лабытнанги
Администрация Тарко-Сале
Private
Cisco 2911
UTP, 1 GE
Помещение серверной
Сервер HP (основной)
Виртуальные роли:
Сервер БД
Сервер DHCP
Сервер Active Directory
Сервер почты IMAP
Сервер данных МСУ-СМАРТ и Реестр
Сервер HP (зеркалирование)
Рубежи защиты серверной:
Отдельное помещение
Пропускной режим
Пожарно-охранная сигнализация
Cisco 2960, 1 эт.
Cisco 2960, 2 эт.
Cisco 2960, 3 эт.
Cisco 2960, 4 эт.
48 портов
UTP, FE
ПК-1.1
ПК-2.1
ПК-3.1
ПК-4.1
ПК – 1.n
ПК – 2.n
ПК – 3.n
ПК – 4.n
Пул IP: 167.117.12.0/24
Администрация Новый Уренгой
Мкрн. Советский, 3

Рисунок 1.1

1.5 Целеполагание проекта информационной безопасности

Основной задачей ВКР является разработка мер и решений по обеспечению информационной безопасности (ИБ) операционной деятельности локальной сети администрации города Новый Уренгой и установлению режима непрерывности предоставления услуг населению.

Анализируя собранную информацию, стоит сказать, что мер и решений по обеспечению информационной защищенности локальной сети администрации города Новый Уренгой в целом недостаточно. Отчасти это сделано потому, что в политиках безопасности прописаны только основные политики и регламенты не в полной мере отражающие все аспекты деятельности муниципальной организации.

Подводя итог оценке и анализу проекта, можно заключить, что в ВКР решается ряд задач:

– определение назначения и функций системы безопасности ЛВС;

– представить перечень функций ИВС;

– выработать базовую модель угроз безопасности;

– рассмотреть основные требования к комплексу технических и программных средств защищенной локально-вычислительной сети (ЗЛВС);

– рассмотреть систему внедрения программного комплекса учета действий за сотрудниками администрации.

Результат анализа локальной инфраструктуры администрации города Новый Уренгой, сведены в таблицу 1.1.

Таблица 1.1 - Исходные данные для проектирования ЗЛВС администрации

Показатель	Значение
Назначение	ИС для автоматизации электронного документооборота
Количество рабочих групп (департаменты)	8
Расстояние между соседними группами, м	50-80
Число рабочих станций в группе - мин/макс, шт.	15/30
Размеры зданий (длина×ширина), м	120*40
Количество этажей/расположенных групп в здании	4
Количество зданий в организации/расстояние между ними, м	1/0

Выводы по разделу один

Подводя итог раздела ВКР и анализируя собранную информацию о структурном составе и операционной деятельности администрации города Новый Уренгой, принято решение предпринять меры по повышению защищенности муниципальной организации в целом [9].

Сами меры планируется разделить на две составляющие:

– организационно-правовые меры;

– технические меры.

К организационно-правовым мерам будут относиться:

– решения по внедрению режима наблюдения и доступности к нормативной и финансовой документации и ограничения лиц, имеющих доступ к изменению данной информации;

– принятие процедуры по оповещению администратора ИБ о критических сбоях в работе информационных систем с помощью SMS;

– ограничить доступ должностных лиц, имеющих доступ к USB портам на рабочих станциях;

– проведение обучения и повышения квалификации администратора ИТ с целью повышения компетенций в сфере ИБ;

– определение порядка учета, выдачи, использования и хранения съемных электронных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные.

К техническим мерам будут относиться [10]:

– решения по реорганизации проводной сети, выделения ее в отдельный адресный пул с присвоением компьютерам MAC ACL;

– ограничение доступа сотрудников и посторонних лиц к техническим средствам локальной сети;

– предотвращение несанкционированного подключения к проводной локальной сети;

– введение режима закрытого доступа в помещение серверной и обеспечение безопасности телекоммуникационного шкафа;

– введение пропускного режима по средствам систем СКУД в технические помещения и серверную;

– мониторинг, аудит и устранение слабых, технически незащищенных мест в существующей инфраструктуре администрации города Новый Уренгой;

– внедрение программного комплекса учета деятельности сотрудников.

Принятие проектных мер позволит повысить информационную безопасность и обеспечит режим надежной и непрерывной работы администрации города Новый Уренгой в целом.

В администрации города Новый Уренгой основным приоритетом является безопасность сервисов, сетей связи, специализированного ПО для госсектора, базы данных ПО, серверов, компьютеров сотрудников, данных населения.

Для государственных муниципальных учреждений особенно важно выполнение нормативно технических и нормативно-правовых актуальных требований. Также особое значение принимает постоянный контроль за соблюдение режима безопасности. Для этих задач в проекте планируется разработать опросные листы, позволяющие более удобно проводить регламентированный регулярный аудит ИБ.

2 АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АДМИНИСТРАЦИИ

2.1 Постановка задачи

В данной главе планируется произвести аудит информационной безопасности администрации, характеристику системы Microsoft Security Assessment Tool, оценку информационной безопасности на предпроектном этапе, оценку уровня организационных мер защиты администрации, анализ полученных результатов оценки ИБ администрации.

2.2 Характеристика системы Microsoft Security Assessment Tool

Для того, чтобы выявить проблемные и слабозащищенные места информационной безопасности существуют специальные программные комплексы, позволяющие упростить процесс оценки. Одной из самых распространенных является система оценки безопасности Microsoft Security Assessment Tool (MSAT) [11].

Выбор данной системы в качестве оценки ИБ администрации основывается на ряде факторов:

– система MSAT позволят получить полностью аналитический расчет по всем деструктивным параметрам и видам воздействия на инфраструктуру предприятия;

– система MSAT предоставляет развернутый отчет с оценкой ИБ, и хранит его. При регулярной проверке позволяет сравнить полученные отчеты с предыдущей версией и сделать вывод;

– система проста в обращении и не требует особых навыков от оператора;

– система полностью бесплатна и доступна на Windows платформе.

Инструмент оценки безопасности Microsoft Security Assessment Tool (MSAT) - это бесплатное средство, разработанное чтобы помочь организациям оценить уязвимости в ИТ-средах, предоставить список расставленных по приоритетам проблем и список рекомендаций по минимизации этих угроз. MSAT - простой, экономичный способ приступить к усилению безопасности вычислительной среды предприятия. В корпорации Microsoft основным приоритетом является безопасность сетей, бизнес-серверов, компьютеров конечных пользователей, мобильных устройств и данных клиентов.

Средство MSAT применяет целостный подход к измерению уровня безопасности и охватывает такие темы, как персонал, процессы и технологии. Система MSAT предоставляет следующие возможности:

– исчерпывающую и постоянную осведомленность об уровне ИБ;

– инфраструктуру эшелонированной защиты, соответствующую отраслевым стандартам;

– подробные, постоянные отчеты, сравнивающие базовые показатели с достигнутыми успехами;

– проверенные рекомендации и расставленные по приоритетности действия для улучшения безопасности.

Оценка состоит из более чем 200 вопросов, разбитых на категории:

– инфраструктура;

– приложения;

– эксплуатация;

– персонал.

Вопросы, составляющие опросную часть средства, и связанные с ними ответы извлечены из общепринятых практических рекомендаций по безопасности как общих, так и конкретных. Предлагаемые вопросы и рекомендации основаны на стандартах ISO 17799 и NIST-800.x [11].

2.3 Оценка информационной безопасности на предпроектном этапе

Анализ информационной защищённости администрации города Новый Уренгой произведен автоматизированным комплексом MSAT. Оценка выполнятся до принятия организационных мер с целью выяснения начальных условий по ИБ администрации.

Результаты отчета, полученного в ходе автоматической оценки ИБ комплексом MSAT, представлены на рисунке 2.1.

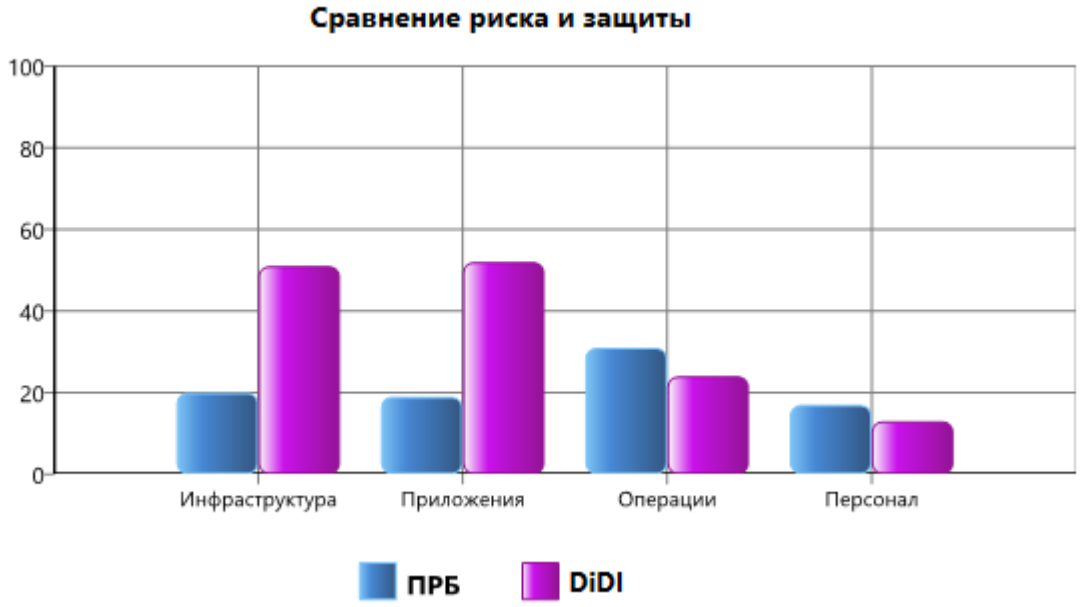

Рисунок 2.1 – Отчет, результирующий анализ информационной безопасности

Показатель ПРБ находится в диапазоне от 0 до 100, где более высокая оценка подразумевает более высокий показатель потенциального риска для бизнеса в данной специфической области анализа (AoA). Важно отметить, что нулевое значение в данном случае невозможно, так как деловая деятельность сама по себе подразумевает наличие какого-то уровня риска. Кроме того, важно понимать, что существуют определенные аспекты ведения бизнеса, для которых отсутствует прямая стратегия снижения риска.

Индекс DiDI также находится в диапазоне от 0до 100. Высокий показатель свидетельствует о среде, в которой было принято множество мер для развертывания стратегий эшелонированной защиты (DiD) в конкретной области (AoA). Показатель DiDI не отражает общей эффективности безопасности или же ресурсы, затраченные на безопасность. Низкий показатель ПРБ и высокий показатель DiDI это хороший результат [15].

Профиль защиты инфраструктуры администрации города Новый Уренгой представлен на рисунке 2.2.

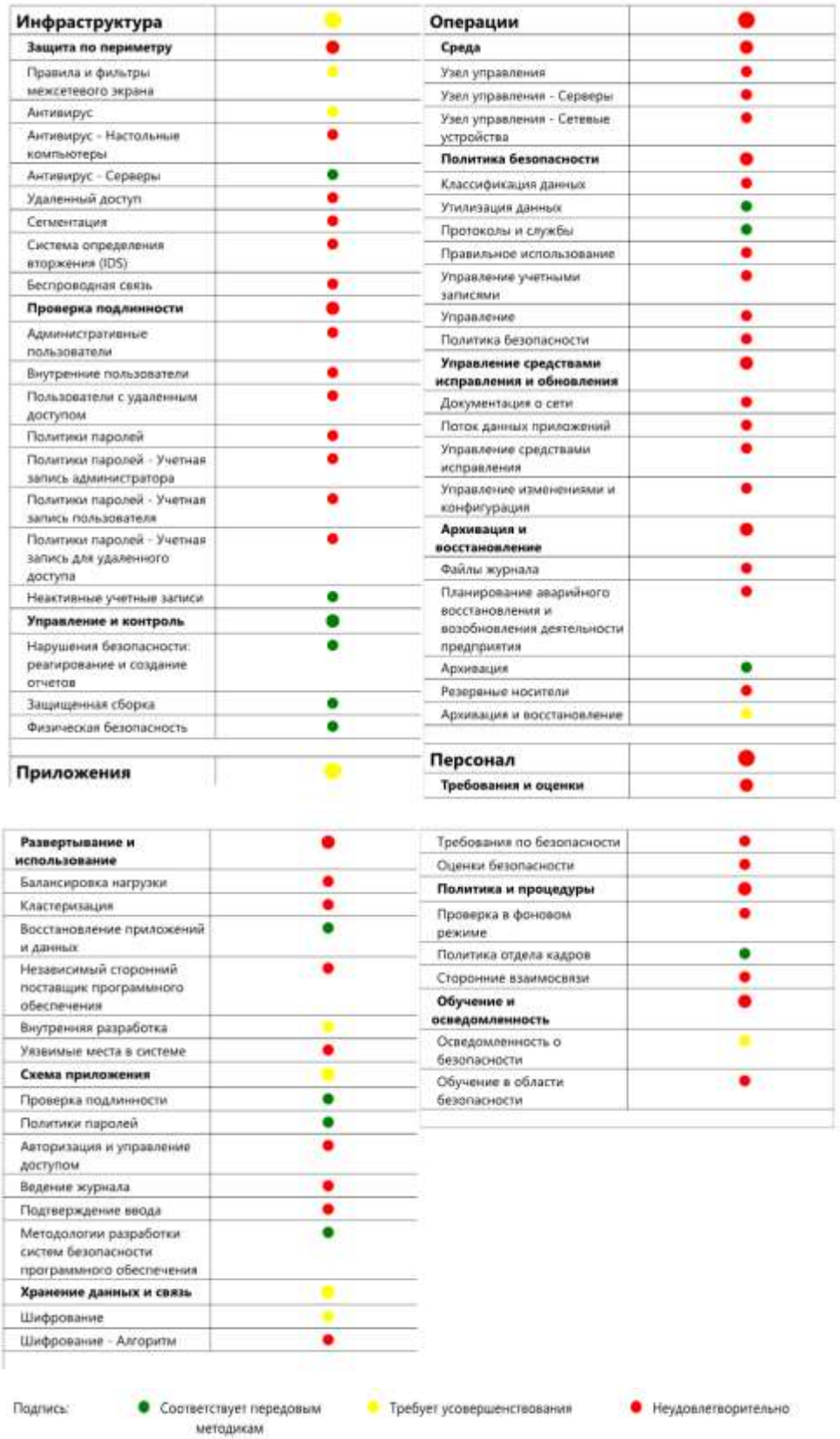

Рисунок 2.2 – Профиль защиты инфраструктуры администрации города

2.4 Оценка уровня организационных мер защиты администрации

В настоящее время, в администрации города Новый Уренгой приняты следующие процедуры и регламенты информационной безопасности.

1) Ограничение доступа работников к персональным данным

Ограничение доступа сотрудников администрации к ПДн - неотъемлемая часть мероприятий по обеспечению безопасности ПДн при их обработке в информационных системах.

Для соблюдения концепции информационной безопасности в администрации приняты меры:

– разработаны функциональных обязанностей должностных лиц службы информационной безопасности;

– создан ряд документов в форме приказов и распоряжений руководства департаментов по вопросам регламентации отношений с населением и контрагентами;

– определены мероприятия по разработке правил управления доступом к внутрисетевым ресурсам (база данных программ госсектора);

– в служебные помещения организован надежный пропускной режим;

– организацию учета, хранения, использования и уничтожения документов и носителей с закрытой информацией (при необходимости).

Данные меры носят обязательный характер для всех отделений и филиалов, работающих на территории России.

2) Документальное регламентирование работы с ПД

В администрации все сотрудники при оформлении на работу ознакомлены под роспись с документами, которые устанавливают порядок обработки персональных данных клиентов, как физических, так и юридических лиц.

3) Согласия на обработку персональных данных физических лиц

В соответствии со статьей 9 ФЗ-№152 «О персональных данных» в администрации города обработка ПДн сотрудника, контрагента или граждан осуществляется только при условии наличия его письменного согласия с указанием данных [26]:

– фамилия, имя, отчество и адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– фамилия, имя, отчество и должность оператора, получающего согласие субъекта ПДн;

– цель обработки ПДн;

– порядок обработки и хранения ПДн;

– перечень ПДн, на обработку которых дается согласие субъекта ПДн;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

– срок, в течение которого действует согласие и порядок его отзыва.

2.5 Анализ полученных результатов оценки ИБ администрации

Анализируя полученные данные, можно заключить, что инфраструктура в целом защищена недостаточно хорошо, однако этому есть ряд объяснений:

– организация большая и нуждается в надёжной защите всех бизнес процессов (особо критические приложения и массивы информации защищены);

– чтобы соответствовать всем международным критериям, необходимо внедрить передовые решения и методы, что в свою очередь очень дорого, а для госучреждений достаточно долго;

особо важные узлы сети защищены, а также обеспечена базовая защита компьютеров установкой современных файрволов и антивирусов.

3 АНАЛИЗ ЦЕЛЕНАПРАВЛЕННЫХ АТАК НА ИНФРАСТРУКТУРУ ИТ И ИБ АДМИНИСТРАЦИИ

3.1 Постановка задачи

В данной главе планируется произвести анализ целенаправленных атак на инфраструктуру ИТ и ИБ администрации, рассмотреть базовую модель угроз безопасности, произвести анализ проблем информационной безопасности администрации, рассмотреть меры и решения защиты от атак.

3.2 Обзор базовой модели угроз безопасности

Для того что бы разработать меры защиты администрации города Новый Уренгой, необходимо определить потенциальные угрозы и возможные пути проникновения нарушителя, то есть рассмотреть модель угрозы объекта.

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций, а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которое ведет к ущербу жизненно важных интересов личности, общества и государства [12].

Модель угроз содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационных системах персональных данных (ИСПДн) администрации, связанным:

– с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;

– с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств, с целью уничтожения или блокирования ПДн [12].

Модель угрозы безопасности представлена на рисунке 3.1 [12].

Рисунок 3.1 - Обобщенная схема канала реализации угроз безопасности персональных данных

Основными элементами ИСПДн являются администрации города Новый Уренгой:

– персональные данные, содержащиеся в базах данных администрации;

– информационные технологии, применяемые при обработке ПДн;

– компьютеры и сервера, осуществляющие обработку ПДн, средства и системы передачи данных;

– программные средства (операционные системы, СУБД);

– средства защиты информации;

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн [12].

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

– источник УБПДн - субъект, материальный объект или физическое явление, создающие УБПДн;

– среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

– носитель ПДн - физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

При взаимодействии с системами обработки информации в администрации города возможны следующие каналы утечки:

– угрозы утечки информации по техническим каналам;

– угрозы утечки акустической (речевой) информации;

– угрозы несанкционированного доступа к информации в информационной системе персональных данных;

– угрозы доступа к данным, используя методы социальной инженерии.

Приведенные выше виды угроз отражают не полную картину опасностей инфраструктуры администрации города Новый Уренгой, однако, эти самые уязвимые места, требующие дополнительного эшелона защиты.

3.3 Анализ проблем информационной безопасности администрации

За 2014-2017 годы увеличилось число попыток проникновения в сетевую инфраструктуру администрации, в том числе и способом APT. Атака APT – это целенаправленная сетевая атака, при которой атакующий пытается получить неавторизованный доступ в сеть администрации и остается необнаруженным в течение длительного времени. При таких атаках, киберзлоумышленники используют методы социальной инженерии и собственные инструменты для эксплуатации уязвимостей.

Традиционные средства защиты (файрволы и антивирусные комплексы) анализируют сигнатуры для обнаружения известных атак и уязвимостей. Однако эти средства не обнаруживают атаки при использовании злоумышленниками неизвестных уязвимостей или методов социальной инженерии.

В настоящее время системы защиты сетевой инфраструктуры государственного сектора ЯНАО и администрации города Новый Уренгой в частности используют традиционные средства защиты, такие как анализ аномалий. Установленная система IDS/IPS, анализирует сетевые аномалии, и может обнаруживать атаки APT. Система IDS/IPS собирает трафик посредством протоколов NetFlow, sFlow, cFlow с сетевых устройств и сравнивает его с «разрешенным/обычным» сетевым трафиком, имевшим место в течение дня, недели, месяца. Однако решения IDS/IPS на основе анализа аномалий подвержены ошибкам [10]:

– false positives - ошибка, при которой нормальный трафик принимается за атаку;

– false negatives - ошибка, при которой атака воспринимается как нормальный трафик.

Ключевые характеристики решения IDS/IPS:

– выявление вредоносного кода, который не могут обнаружить антивирусы, МЭ, системы IDS/IPS и другие средства защиты;

– контроль всех каналов распространения вредоносного ПО: Web, e-mail, HDD, DVD, USB, LAN;

– отсутствие ложных срабатываний;

– собственная система виртуализации для выявления признаков вредоносной активности, при этом файлы из вашей сети не передаются для анализа в облако;

– наличие централизованной системы управления;

– выявление вредоносного кода, который уже присутствует в сети.

Несмотря на то, что при проведении целенаправленных атак методы эксплуатации уязвимостей различаются, сами атаки включают в себя этапы:

– эксплуатация уязвимости;

– загрузка вредоносного кода;

– связь с сервером управления;

– дальнейшее распространение атаки;

– передача конфиденциальной информации.

Эксплуатация уязвимости обычно происходит через Web-браузер, когда сотрудник, попадая на сайт злоумышленника, активирует закладку с помощью JavaScript или, например, просмотра JPG-картинки или видео. Возможно заражение компьютера с помощью сообщения электронной почты, когда передается гиперссылка, ведущая на фишинговый сайт, или вложение, Excel или PDF. Когда сотрудник кликает мышью по гиперссылке или файлу вложения, открывается Web-браузер или другое приложение Adobe Reader, Microsoft Excel. Гиперссылка может использовать скрытый адрес. После его раскодирования компьютер жертвы устанавливает соединение с сервером атакующего, откуда загружается вредоносное ПО (за период с 2016-2017 года в администрации города Новый Уренгой зафиксировано 142 случая проникновения зловредного кода и заражения компьютеров сотрудников). После этого вредоносное ПО устанавливает шифрованное соединение с сервером управления (с помощью SSL). Это позволяет киберпреступнику обходить традиционную защиту, предлагаемую МЭ и системами обнаружения вторжений, которые не могут идентифицировать команды и данные, передаваемые в зашифрованном виде.

Так как администрации города Новый Уренгой недостаточно защищена от целенаправленных атак, это зачастую приводит к последствиям:

- Ответственность за несоблюдение законодательных требований. Ответственность предусмотрена российскими и зарубежными требованиями стандартов и законодательства (ФЗ, защита ПДн, КВО, требования ЦБ РФ, стандарты PCI DSS, SoX и прочие).

- Ущерб репутации. Доверие со стороны граждан и контрагентов важно во всех госструктурах. В 2018 году ущерб репутации оценивается в несколько миллионов рублей [5].

- Остановка операционной деятельности и работы администрации. После успешной атаки не так просто восстановить системы в доверенное состояние, если они не допускают перерывов в работе.

3.4 Меры и решения защиты от атак

Некоторые решения по защите от вышеприведенных атака на сетевую инфраструктуру администрации города Новый Уренгой приняты, однако они не отрабатывают все виды угроз, и самое важное они не защищают от действий социальной инженерии. Чтобы успешно противостоять таким атакам, решение должно уметь обнаруживать и блокировать вредоносную активность на каждом этапе по следующему алгоритму [2].

Шаг 1: система анализирует входящий и исходящий трафик, проверяя наличие известных атак, установление соединений с серверами управления. Если известная атака или связь с сервером управления обнаружена, система блокирует соединение.

Шаг 2: для атак нулевого дня система помещает файлы или Web-страницу в виртуальную среду для анализа.

Шаг 3: в виртуальной среде запускаются различные версии операционной системы Microsoft Windows и приложений Microsoft Office, Microsoft Edge, Adobe Reader, специализированное ПО и другие. С их помощью обрабатываются подозрительные файлы и Web-ссылки. При обнаружении атаки, изменения в корневом разделе файловой системы, попытки установления соединения с сервером СУБД – виртуальная машина перезапускается.

Шаг 4: если подтверждается атака нулевого дня, система записывает последующие действия вредоносного ПО. На основе полученных данных система формирует новый профиль защиты для блокирования ставшей уже известной атаки.

Шаг 5: новый профиль защиты передается на другие компьютеры, которые находятся в сети администрации.

Данное решение, планируется развернуть как виртуальная роль на сервере в администрации города Новый Уренгой, которое, по сути, будет отрабатывать большинство целенаправленных атак. Однако данное решение не обеспечивает все рубежи защиты и не гарантирует полную защиту от киберперступлений.

4 РАЗРАБОТКА ОПРОСНЫХ ЛИСТОВ ПО ОЦЕНКЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ

4.1 Постановка задачи

В данной главе планируется разработать опросные листы по оценке выполнения требований безопасности, рассмотреть этапы разработки методики оценки, произвести анализ нормативных источников в сфере Госуслуг, определить критерии оценки на основании анализа источников, разработать вопросы опросного листа, автоматизировать оценки соответствия ИБ организации.

4.2 Этапы разработки методики оценки

Для начала разработки проекта защиты инфраструктуры администрации, необходимо провести комплексную оценку существующего состояния. С целью проведения процесса аудита ИБ, в проекте принято решение в разработке опросных листов, которые позволяют провести комплексную оценку и выявить слабые места.

Разработка инструмента по оценки соответствия информационной безопасности организаций отраслевым требованиям решается последовательным выполнением следующих задач [2]:

– сбор и анализ актуальных нормативных документов;

– осуществление выбора критериев для степени соответствия сформированным актуальным требованиям по обеспечению информационной безопасности организации (соответствия);

– разработка опросных листов для оценки соответствия;

– разработка процедуры оценки соответствия;

– разработка программы, реализующей оценку соответствия

– проведение оценки информационной безопасности администрации.

4.3 Анализ нормативных источников в сфере Госуслуг

Среди всего многообразия документов и стандартов в сфере информационной безопасности для качественной оценки администрации города Новый Уренгой выбраны регламенты, представленные ниже.

1) ГОСТ Р-27001-2006. Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

В документе регламентируются:

– требования в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности (СМИБ);

– требования к системе менеджмента информационной безопасности для демонстрации организации защищать информационные ресурсы;

– методы и средства обеспечения безопасности;

– требования к документированию;

– политика ответственности;

– проведение внутренних аудитов;

– цели и механизмы контроля.

Стандарт ГОСТ Р ИСО/МЭК 27001-2006 является признанным стандартом в области построения Системы Управления Информационной Безопасностью (СУИБ) организации, универсальность данного стандарта позволяет использовать его во всех типах организаций вне зависимости от профиля их деятельности. ГОСТ Р ИСО/МЭК 27001-2006 включает в себя требования для разработки и эксплуатации системы управления информационной безопасности организации.

Требования, изложенные в этом Международном стандарте, носят общий характер и предназначены для применения в любых организациях, независимо от их типа, размера или области деятельности [14].

2) ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Компоненты доверия к безопасности.

В документе регламентируются:

– основные принципы и подходы к установлению доверия к безопасности, позволяет понять логику построения требований доверия;

– четкое формулирование угрозы безопасности и положения политики безопасности организации;

– излагает концепцию формулировки, принципы обеспечения доверия.

Данный документ относится к базовым и описывает общие понятия угрозы и информационного доверия. К данному проекту носит рекомендательный характер. В госсекторе используется много специально разработанного ПО, разработка, сертификация и внедрение которого необходимо проверять на

киберзащищенность на каждом этапе. Данный ГОСТ регламентирует методы и средства обеспечения безопасности, в том числе и специализированного ПО [15].

3) ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

В документе регламентируются:

– руководство по менеджменту риска информационной безопасности (ИБ) в организации, поддерживая, в частности, требования к системе менеджмента информационной безопасности (СМИБ) в соответствии с ИСО/МЭК 27001;

подробно описан процесс менеджмента риска информационной безопасности.

Настоящий стандарт не предоставляет какой-либо конкретной методологии по менеджменту риска информационной безопасности. Относится к базовым основополагающим документам [16].

4) ГОСТ Р МЭК 61508-3-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных связанных с безопасностью. Требования к программному обеспечению.

В документе регламентируются:

– устанавливает метод разработки спецификации требований к безопасности, необходимых для достижения заданной функциональной безопасности Э/ПЭ систем, связанных с безопасностью;

– применяет для определения требований к уровням полноты безопасности подход, основанный на оценке рисков [17].

5) ГОСТ Р ИСО/МЭК ТО 19791-2008. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

В документе регламентируются:

– определение и модель АС;

– описание расширений концепции оценки безопасности с помощью стандартов серии ИСО/МЭК 15408, необходимых для оценки АС;

– методологию и процесс выполнения оценки безопасности АС;

– дополнительные критерии оценки безопасности, охватывающие те аспекты АС, которые не были охвачены критериями оценки безопасности в стандартах серии ИСО/МЭК 15408.

Настоящий стандарт, ограничивается оценкой безопасности автоматизированных систем и не распространяется на другие формы оценки.

Настоящий стандарт содержит рекомендации и критерии оценки безопасности автоматизированных систем и дает возможность включать

продукты безопасности, оцененные в соответствии с требованиями стандартов серии ИСО/МЭК 15408, в автоматизированные системы и проводить оценку как единого целого с использованием настоящего стандарта [18].

6) ГОСТ Р ИСО/МЭК 27002-2012. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности в организациях.

В документе регламентируются:

– описание физической безопасности систем;

– политику информационной безопасности;

– управление доступом;

– безопасность, связанная с персоналом;

– менеджмент инцидентов ИБ;

– менеджмент непрерывности бизнеса;

– организационные аспекты ИБ.

Настоящий национальный стандарт предлагает рекомендации и основные принципы введения, реализации, поддержки и улучшения менеджмента информационной безопасности в организации. Цели, изложенные в данном национальном стандарте, обеспечивают полное руководство по общепринятым целям менеджмента информационной безопасности [19].

7) ГОСТР ИСО 22301 – 2014. Системы менеджмента непрерывности бизнеса. Общие требования.

В документе регламентируются:

– требования к планированию;

– условия организации;

– анализ лидерства;

– планирование и поддержка деятельности бизнеса;

– оценка выполнения организации устойчивости бизнеса;

– постоянное улучшение.

Настоящий стандарт использует модель PDCA для планирования, установления, внедрения, функционирования, мониторинга, поддержки и непрерывного совершенствования результативности СМНБ организации [20].

8) ГОСТ Р 18044-2007. Менеджмент инцидентов информационной безопасности.

В документе регламентируются:

– ключевые вопросы менеджмента инцидентов ИБ;

– планирование и подготовка;

– использование, оценка и принятие решений по событиям/инцидентам;

– анализ и мониторинг менеджмента инцидентов ИБ;

– улучшение анализа рисков менеджмента ИБ.

Положения настоящего стандарта содержат представление о менеджменте инцидентов информационной безопасности в организации с учетом сложившейся практики на международном уровне [21].

9) Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

В документе регламентируются:

– осуществление права на поиск, получения, передачу, производство и распространение информации;

– применение информационных технологий;

– обеспечение защиты информации.

Закон регламентирует все организационно-правовые отношения в сфере информатизации и защиты информации [22].

10) Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

В документе регламентируются:

– принципы и условия обработки данных;

– права субъекта персональных данных;

– контроль и надзор за обработкой персональных данных;

– ответственность за нарушение требований настоящего ФЗ.

Закон регламентирует отношения, связанные с обработкой персональных данных, осуществляемой государственными органами, юридическими лицами, физическими лицами при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в субъекте Российской Федерации [23].

11) Нормативно-методический документ ФСТЭК России от 15.02.2008 «Об утверждении Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

В документе регламентируются:

– описание модели угроз ПД при их обработке ИС;

– принципы защиты персональных данных.

В документе приведена постановка задачи по созданию базовых моделей угроз и методов негативного воздействия на информацию, а также приказы 17 и 21 [24].

4.4 Определение критериев оценки на основании анализа источников

Из списка нормативных документов выбран Эталон документ, наиболее полно отражающий структуру оценки соответствия ИБ:

ГОСТ Р ИСО/МЭК 27002-2012. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности в организациях [19].

Защита информации в РФ осуществляется на основании федеральных законодательных нормативных актов, инструкций, постановлений, ГОСТ.

На основе эталонного документа сформирован список критериев оценки соответствия ИБ, с присвоением кода критерия:

– M1 - Система менеджмента ИБ;
– M2 - Защита персональных данных граждан (контрагентов);
– M3 - Управление доступом;
– M4 - Физическая безопасность;
– M5 - Безопасность, связанная с сотрудниками;
– M6 - Оценка риска;
– M7 - Обеспечение рабочих процессов;
– M8 - Управление инцидентами.

Степень описания критерия в тексте представлена в графическом формате:

	детальное описание данного критерия присутствует в данном документе;
	описание данного критерия не достаточно полное в данном документе;
	данный критерий присутствует в данном документе, но нет его описания;
	данный критерий отсутствует в тексте данного документа.

Формирование таблицы оценки описания критериев представлено таблицы А.1 (Приложение А).

В таблице А.1 проведена оценка критериев, описанных в документах. Оценка степени описания критерия в тексте Источника осуществляется по принципу:

– есть/нет данный критерий в тексте;

– если есть, то насколько полно рассмотрены положения данного критерия.

4.5 Разработка вопросов опросного листа

Для каждого нормативного источника в рамках одного критерия сформирован список вопросов, при ответе на которые можно оценить выполнение требований критерия.

Так как в разных нормативных документах возможно описание критерия и его положений с одной и той же позиции, что вызовет формирование одинаковых вопросов, то необходимо сформировать общую базу вопросов, в которой будет исключена возможность их повторения. Общий список вопросов представлен в формате таблицы.

Таблица 4.1 – Вопросы критерия «М1 – Система менеджмента ИБ»

№ воп.	Источник	Вопросы к критерию	Обязательность (да/нет)	Коэф. знач.
1	ГОСТ Р-27001-2006 ГОСТ Р 15408-3-2013	Обозначены ли требования к разработке СУИБ?	да	0,3
2	ГОСТ Р-27001-2006	Осуществляется ли постоянный контроль за выполнением требований ИБ?	да	0,2
3	ГОСТ Р-27001-2006 ГОСТ Р 18044-2007	Определена ли ответственности сотрудников администрации за невыполнение требований ИБ?	да	0,1
4	ГОСТ Р-27001-2006	Предусмотрен ли аудит СУИБ?	нет	0,05
5	ГОСТ Р-27001-2006 ФЗ № 149 от 27.07.06	Предусмотрено ли постоянное улучшение организации СУИБ?	нет	0,1
6	ГОСТ Р 27002-2012 ГОСТ Р 15408-3-2013	Прописаны ли требования к ведению документации ИБ?	да	0,2
7	ГОСТ Р 27002-2012 ГОСТ Р 15408-3-2013	Защищены ли результаты аудита от внешнего доступа к ним?	нет	0,05

Таблица 4.2 – Вопросы критерия «М2 - Защита персональных данных граждан (контрагентов)»

№ воп.	Источник	Вопросы к критерию	Обязательность (да/нет)	Коэф. знач.
1	ФЗ № 149 от 27.07.06	Прописан ли регламент обработки ПДн?	да	0,2
2	ФЗ № 152 от 27.07.06	Соблюдение требований обеспечения ИБ ПДн?	да	0,3
3	Норм. мет. док. ФСТЭК России от 15.02.2008	Осуществляется ли контроль за сотрудниками ответственными за защиту ПДн?	да	0,1
4	*	Прописаны ли правила архивного хранения ПДн?	нет	0,05
5	ФЗ № 149 от 27.07.06 Норм. мет. док. ФСТЭК России от 15.02.2008	Считается ли нарушение режима защиты ПДн грубым проступком и приводит к дисциплинарной ответственности?	да	0,1
6	ФЗ № 149 от 27.07.06 ФЗ № 152 от 27.07.06	Гарантирована ли конфиденциальность ПД на всех этапах обработки ПД?	да	0,15
7	Пост. Прав. от 16.04.2012 г. № 313 ФЗ № 149 от 27.07.06	Формируется ли перечень документов, содержащих ПД?	нет	0,1

Таблица 4.3 – Вопросы критерия «М3 – управление доступом»

№ воп.	Источник	Вопросы к критерию	Обязательность (да/нет)	Коэф. знач.
1	ГОСТ Р-27001-2006 Норм. мет. док. ФСТЭК России от 15.02.2008	Рассматриваются ли уровни доступа к ИСПД?	да	0,1
2	ФЗ № 149 от 27.07.06	Приняты ли меры по ограничению доступа посторонних лиц к ИСПД?	да	0,3
3	ГОСТ 22301-2014 ГОСТ Р 27002-2012 ФЗ № 149 от 27.07.06	Осуществляется ли контроль за соблюдение режима доступности?	да	0,2
4	ГОСТ 22301-2014	Предусмотрена ли автоматизированная система ограничения доступа?	нет	0,05

Продолжение таблицы 4.3

5	ФЗ № 149 от 27.07.06	Внедрена ли политика ограничения доступа к к ИСПД?	да	0,1
6	ГОСТ Р 27002-2012	Предусмотрена ли ответственность за нарушение режима доступа к ИСДП?	да	0,2
7	ГОСТ Р 27002-2012 ФЗ № 149 от 27.07.06	Регламентируются ли порядок расследования нарушения контроля доступа?	нет	0,05

Таблица 4.4 – Вопросы критерия «М4 - Физическая безопасность»

№ воп.	Источник	Вопросы к критерию	Обязательность (да/нет)	Коэф. знач.
1	ГОСТ Р 27002-2012	Степень защищенности материальных фондов?	да	0,3
2	ГОСТ Р-27001-2006 ГОСТ Р 27002-2012	Регламентируется ли специальная проверка компонентов СКУД?	нет	0,1
3	ГОСТ Р 27002-2012	Предусмотрены ли меры по препятствию вторжения в системы связи (закладки, сканирование диапазона)?	да	0,3
4	ГОСТ Р 61508-3-2012	Предусмотрена ли система о предупреждении о атаке?	нет	0,05
5	ГОСТ Р 27002-2012	Обозначены ли функциональные требования к защите технических систем?	да	0,1
6	ГОСТ Р 61508-3-2012 ГОСТ Р 15408-3-2013	Рассматриваются ли требования экономической целесообразности к защите технических систем?	нет	0,05
7	ГОСТ Р 27002-2012	Разработана ли инструкция по мерам противодействия злоумышленникам?	да	0,1

Таблица 4.5 – Вопросы критерия «М5 – Безопасность, связанная с сотрудниками»

№ воп.	Источник	Вопросы к критерию	Обязательность (да/нет)	Коэф. знач.
1	ГОСТ Р 61508-3-2012 ГОСТ Р 27005-2010	Проводится ли проверка персонала перед устройством на работу?	да	0,2

Продолжение таблицы 4.5

2	ГОСТ Р 61508-3-2012 ГОСТ Р 27005-2010	Предусмотрена ли административная ответственность персонала за нарушение конфиденциальности?	да	0,4
3	ГОСТ Р 61508-3-2012 ГОСТ Р-27001-2006	Предусмотрены ли меры и средства контроля за персоналом?	да	0,2
4	ГОСТ Р 61508-3-2012 ГОСТ Р-27001-2006	Проводится ли обучение персонала в области ИБ?	да	0,05
5	ГОСТ Р 61508-3-2012	Ведется ли мониторинг за действиями сотрудников, работающих с ПД?	да	0,05
6	ГОСТ Р 61508-3-2012	Прописаны ли обязанности руководства по надлежащему контролю в сфере ИБ?	да	0,05
7	ГОСТ Р 27005-2010 ГОСТ Р 18044-2007	Отражает ли регламент работы политику ИБ?	нет	0,05

Таблица 4.6 – Вопросы критерия «М6 – Оценка риска»

№ воп.	Источник	Вопросы к критерию	Обязательность (да/нет)	Коэф. знач.
1	ГОСТ Р 27005-2010	Принят ли регламент оценки рисков?	да	0,3
2	ГОСТ Р 27005-2010	Проводится ли ежегодный аудит ИБ?	да	0,2
3	ГОСТ Р 18044-2007 ГОСТ Р 18044-2007	Разработаны ли шкалы оценки риска?	да	0,1
4	ГОСТ Р 15408-3-2013	Проводится ли работа по улучшению и уточнению оценки по уже выявленным инцидентам?	нет	0,1
5	ГОСТ Р 27005-2010	Учитывается при оценке рисков заключения экспертов сферы ИБ?	нет	0,1
6	ГОСТ Р 27005-2010	Учтена ли процедура оценки рисков в документах нормативной базы администрации?	нет	0,1
7	*	Утверждена ли методика оценки рисков ИБ в ФСБ/ФСЭК?	нет	0,1

Таблица 4.7 – Вопросы критерия «М7 - Обеспечение непрерывности рабочих процессов»

№ воп.	Источник	Вопросы к критерию	Обязательность (да/нет)	Коэф. знач.

1	ГОСТ 22301-2014 ГОСТ Р 19791-2008	В ИС прописаны требования к непрерывности рабочих процессов (НРП)?	да	0,2
2	ГОСТ 22301-2014 ГОСТ Р 27002-2012	Применена ли система управления непрерывности рабочих процессов?	да	0,2
3	ГОСТ 22301-2014 ГОСТ Р 27002-2012	Проводится ли контроль непрерывности рабочих процессов?	да	0,1
4	ГОСТ Р 27002-2012	Проводится ли анализ/аудит рисков и благоприятных возможностей?	да	0,2
5	ГОСТ 22301-2014	Проводится ли планирование и контроль деятельности за работоспособностью оборудования сотрудниками?	да	0,1
6	ГОСТ Р 19791-2008	Установлен ли регламент внедрение НРП?	нет	0,1
7	ГОСТ 22301-2014 ГОСТ Р 27002-2012 ГОСТ Р 19791-2008	Планировано ли постоянное улучшение НБ?	да	0,1

Таблица 4.8 – Вопросы критерия «М8 - Управление инцидентами»

№ воп.	Источник	Вопросы к критерию	Обязательность (да/нет)	Коэф. знач.
1	ГОСТ Р 18044-2007 ГОСТ Р 61508-3-2012	Внедрена ли система управления инцидентами?	да	0,4
2	ГОСТ Р 18044-2007 ГОСТ Р 61508-3-2012	Утверждена ли программа менеджмента инцидентов ИБ?	да	0,1
3	ГОСТ Р 18044-2007 ГОСТ Р 61508-3-2012	Обеспечивается ли техническая поддержка пользователей при возникновении инцидентов?	да	0,2
4	ГОСТ Р 18044-2007	Внедрен ли регламент нормативных сроков устранение инцидентов?	нет	0,05
5	ГОСТ Р 61508-3-2012 ГОСТ Р 22301-2014	Присутствует ли система обнаружения и оповещения о событиях ИБ?	да	0,1
6	ГОСТ Р 18044-2007	Внедрена ли система ГосСОПКИ?	нет	0,1
7	ГОСТ Р 61508-3-2012	Предусмотрена ли сотрудник быстрого реагирования на инциденты?	да	0,05

Каждому вопросу из списка выставляем нормированный коэффициент значимости. Значения коэффициентов должны быть такими, чтобы сумма коэффициентов одного критерия была ровна единица. Значения выставляются по степени важности выполнения положения, описанного в вопросе. Чем степень важности выше, тем больше коэффициент значимости. Так же при выставлении значения коэффициента следует указать обязательно ли выполнение данного положения, при этом коэффициент обязательного положения, должен быть выше, чем необязательного. Определить степень важности выполнения положения и обязательность его выполнения помогает источник вопроса, в котором сформулировано данное [13].

4.6 Автоматизация оценки соответствия ИБ организации

В проекте разработан комплекс опросных листов, позволяющих оценивать соответствия уровня ИБ администрации, основанных на списке вопросов и оценке коэффициентов значимости этих вопросов. Комплекс опросных листов создана с целью, чтобы эксперт, которому необходимо оценить соответствие, ответив на вопросы, получил значение оценки соответствия ИБ администрации.

В разрабатываемом комплексе опросных листов оценка соответствия ИБ содержится:

– вывод оценки по соответствию критерия требованиям на базе ответов на вопросы и коэффициентах значимости;

– объединение критериев в логические группы, с выведением оценки каждой группы;

– получение итоговой оценки соответствия на основе оценок логических групп.

Для проверки состоятельности разработанного инструмента его необходимо оформить в виде программы с интерфейсом, содержащим следующие возможности:

– возможность ответить на вопросы (ответы могут быть либо в бинарной форме – да/нет, либо в вероятностной – от 0 до 1) и посмотреть оценки соответствия по каждой логической группе и итоговую оценку соответствия ИБ организации;

– возможность просмотреть логику выведения оценок групп и итоговой оценки.

Комплекс опросных листов разработан средствами Microsoft Excel [13].

Присутствует список вопросов для данного критерия, ответ на вопросы производится в виде выставления «1» в ячейку с соответствующей вероятностью выполнения положения. Так же есть возможность оставить вопрос без ответа, выставив «1» в столбец «Н/О».

После заполнения таблицы одного критерия ответами, появляется итоговая оценка данного критерия. Логика выставления оценки критерия строится на формулах, отображение которых можно настроить в Microsoft Excel, формулы опросных листов представлены в приложении Б.

Итоговые оценки всех критериев сформированы в итоговой таблице в отдельном разделе комплекса опросных листов, где происходит объединение критериев в логические группы и вывод итоговой оценки соответствия ИБ администрации. Результаты оценки итоговой таблицы представлены в приложении Б.

Для оценки соответствия требованиям ИБ администрации необходимо в таблицы критериев М1-М8 (вкладки комплекса опросных листов 1-8) ответить на каждый вопрос, проставляя ответ в соответствующую графу со значащим коэффициентом. Ответ выставляется в вероятностной форме, то есть «1» ставится на необходимой вероятности оценки. Если ответа на вопрос нет, то «1» необходимо проставить в графе Н/О [13].

После ответов на все вопросы во вкладке «Итоговая оценка» автоматически выставляется оценка, в специальном поле, выделенным красной заливкой.

Для проверки корректности работы опросных листов требуется провести оценку соответствия. В результате ответов на поставленные вопросы программа выдает итоговую оценку в зависимости от ответов. По результатам оценки ИБ администрации города Новый Уренгой получено значение: 0,41.

Итоговое значение можно интерпретировать как «низкое», поскольку защите оборудования, линий связи и доступа в серверное помещение уделено недостаточное внимание. Также крайне низкой защитой контроля за деятельностью сотрудников, что влечет риски и большие угрозы со стороны социальной инженерии.

Данные аспекты и были выявлены в ходе выполнения оценки ИБ администрации города Новый Уренгой.

Выводы по разделу четыре

Таким образом, подводя итог к главе, стоит отметить, что в ходе проведения оценки ИБ администрации города Новый Уренгой произведен комплексный

аудит. Полученное значение является отправной точкой и, по сути, является индикатором, показывая какие сферы информационной безопасности требуют усиленной или дополнительной защиты. Защищённость инфраструктуры администрации определяется самым слабым местом, которое, по сути, проведенной комплексной оценке, выявила недостаточный контроль за деятельностью сотрудников администрации, работающих с системой ПДн, то есть канал утечки персональных данных и закрытой информации со стороны социальной инженерии не ликвидирован.

5 РАЗРАБОТКА КОМПЛЕКСА ОРГАНИЗАЦИОННЫХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АДМИНИСТРАЦИИ

5.1 Постановка задачи

В данной главе планируется разработать комплекс организационных мер по обеспечению информационной безопасности администрации, произвести планирование информационной безопасности, рассмотреть повышение квалификации администратора ИТ, произвести процедуру оповещения администратора ИТ о критических сбоях.

5.2 Планирование информационной безопасности

Защита информации включает в себя комплекс мероприятий, направленных на обеспечение информационной безопасности. На практике под этим понимается поддержание целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Основной критерий для выбора уровня защиты - важность информации. Сетевые серверы должны быть расположены в защищенном месте. На каждой рабочей станции должен быть предусмотрен уникальный входной пароль с периодическим обновлением. Для регистрации попыток обращения пользователей к ресурсам следует регулярно проводить аудит сети. С целью предотвращения возможности несанкционированного копирования данных следует использовать бездисковые рабочие станции. Наконец, с этой же целью можно предусмотреть шифрование данных [25].

Для защиты от безвозвратного разрушения данных обычно предусматривают резервное копирование по составленному плану, а также применение резервных источников питания. Права доступа для групп пользователей представлены в таблице 5.2.

Таблица 5.2 - Права доступа для групп пользователей

Название группы	Внутренние ресурсы	Уровни доступа к внутренним ресурсам	Доступ в Интернет и электронная почта
Отдел ИТ	Все сетевые ресурсы	Права администратора в каталогах, в том числе изменение	Все сетевые ресурсы

		уровня и прав доступа	
Финансовая служба	Финансовая информация администрации	Доступ только к специально отведенным областям	Ограничение по IP- адресу (адресата и источника). Идентификация и аутентификация удаленного пользователя Запрет удаленного доступа.
Управления делами	Вся информация администрации	Ограничение доступа к папкам (по необходимости)	Ограничение по IP- адресу (адресата и источника), ограничение по содержанию (входящей и исходящей корреспонденции). Идентификация и аутентификация удаленного пользователя
Название группы	Внутренние ресурсы	Уровни доступа к внутренним ресурсам	Доступ в Интернет и электронная почта
Отделы	Вся информация администрации	Ограничение доступа к папкам (по необходимости)	Ограничение по IP- адресу (адресата и источника), ограничение по содержанию (входящей и исходящей корреспонденции). Идентификация и аутентификация удаленного пользователя
Департаменты	Базы данных разрабатываемых документов	Ограничение доступа к папкам (по необходимости)	Ограничение по IP- адресу (адресата и источника), ограничение по содержанию (входящей и исходящей корреспонденции). Идентификация и аутентификация удаленного пользователя
Отдел информационных технологий	Документация по информационной инфраструктуре	Создание, чтение файлов, запись в файл, создание подкаталогов и файлов, удаление каталогов, поиск файлов, изменение каталогов	Все сетевые ресурсы

В целях защиты ресурсов администрации от распространения вредоносного кода и для снижения рисков утечки конфиденциальных данных утверждается список должностей, для которых предоставляется доступ к USB портам на рабочих станциях/ноутбуках для выполнения служебных обязанностей [3]:

– заместители главы;

– начальники департаментов;

– начальники отдела;

– старший администратор ИТ.

Согласно «Политике информационной безопасности управления ЯНАО, администрация города Новый Уренгой» оставляет за собой право ограничить и отслеживать подключение USB устройств к рабочим станциям.

5.3 Повышение квалификации администратора ИТ

Одной из главных организационных мер, позволяющих повысить уровень ИБ администрации города Новый Уренгой, является специализированное обучение администратора ИТ на курсах по информационной безопасности с получением сертификата. Данная мера позволяет повысить компетенцию и ответственность должностного лица, однако расширит круг его задач. Стоит уточнить, что большая часть задач по обеспечению ИБ соотносится с задачами по организации работоспособности сетевой инфраструктуры и поэтому выполнение работ может быть одновременным. При повышении квалификации администратора ИТ администрации, необходимо также заложить повышение зарплаты, так как вырастает объем выполняемых задач и ответственность за них [26].

Целью обучения должности администратор ИБ является аудит и анализ вопросов информационной безопасности, связанных с эксплуатацией информационных систем и выполнением нормативных требований регулирующих органов.

Администратор ИБ будет проходить курсы по программе Cisco Security в академии Cisco, с получением соответствующего сертификата CCNA с дальнейшей перспективой получения CCNP.

Наиболее распространённый сертификат из всей линейки сертификации Cisco является CCNA. Существует два способа получения сертификата одним экзаменом CCNA Routing and Switching или двумя (ICND1 и ICND2).

После прохождения курсов повышения квалификации в сфере ИБ, на администратора возлагаются следующие обязанности [26]:

– разработка и управление действиями по информационной безопасности администрации;

– определение и внедрение правил и процедур безопасности информационных систем;

– учет и анализ рисков;

– контроль выполнения правил безопасности, установленных IT;

– техническая валидация инструментов безопасности, внедряемых в сферу информационной безопасности;

– консультация и помощь сотрудникам администрации;

– предложение решений для усиления конфиденциальности, целостности и доступности применяемых данных;

– обеспечение информирования всех команд об ИБ;

– гарантия соблюдения политики по информационной безопасности;

– выявление рисков информационной безопасности.

Все принятые организационные меры позволяют повысить уровень информационной безопасности администрации города Новый Уренгой, без вложения существенных капитальных затрат.

5.4 Процедура оповещения администратора ИТ о критических сбоях

Разворачивание системы уведомление в администрации города Новый Уренгой осуществляется путем автоматизированной отправки SMS абонентам, использующим корпоративную мобильную связь (далее – абонентам). Список абонентов и его изменения предоставляются департаменту ИТ.

Уведомление отправляется сервером в любое время суток, в рабочие, выходные и праздничные дни непосредственно после обнаружения критического сбоя. Уведомление может быть отправлено одновременно всем абонентам или выборочно.

Под критическим сбоем понимается продолжительное (более 15 минут) нарушение работы следующих ИТ сервисов:

– корпоративная почта;

– общие сетевые ресурсы;

– каналы передачи данных;

– корпоративные информационные системы;

– Front Office;

– Active Directory;

– сетевая и серверная инфраструктура, в том числе нарушения электропитания и условий функционирования;

– телефония, беспроводные сети и системы телеконференций;

– иные, затрагивающие всех пользователей.

При обнаружении критического сбоя сервер поддержки определяет список абонентов и инициирует уведомление с помощью ITSM системы.

Уведомление составляется на русском языке с использованием шаблона, включает в себя краткое описание проблемы и приблизительное время решения.

Перед отправкой уведомление подтверждается администратором ИТ, после чего автоматически отправляется абонентам.

При восстановлении работы сервиса после критического сбоя или изменения информации, содержащейся в предыдущем оповещении, осуществляется повторное оповещение.

6 РАЗРАБОТКА КОМПЛЕКСА ТЕХНИЧЕСКИХ МЕР ПО ИНФОРМАЦИОННОЙ ЗАЩИТЕ АДМИНИСТРАЦИИ

6.1 Постановка задачи по проектируемым мерам

Согласно проведенному аудиту предпроектного состояния и выявления слабозащищенных мест, выявленных в главе 2 и 3, в данном проекте планируется внедрить ряд технических мер с целью повышения уровня информационной и структурной защищенности администрации в целом.

К мерам технического характера относится:

– разработка процедуры блокировки учетных записей сотрудников;

– разработка процедуры оповещения администратора ИТ о технических сбоях и инцидентах безопасности;

– разворачивание системы СКУД, с целью ввести пропускной режим с учетом рабочего времени сотрудников;

– реорганизация локальной вычислительной сети администрации;

– внедрение специализированного программного решения для госсектора, производящего мониторинг и учет за действиями сотрудников на ПК.

6.2 Выбор системы блокировки учетных записей сотрудников

В администрации города Новый Уренгой для управления учетными записями пользователей планируется внедрить ITIM (IBM Tivoli Identity Management). Данное решение устанавливается согласно приказа управления администраций ЯНАО. Для этих целей необходимо настроить интеграцию ITIM со следующими системами:

– HR Access (приложение отдела персонала для ведения данных по сотрудникам администрации);

– Active Directory (AD) – учетная запись пользователя в домене госсектора;

– учетная запись EasyMail (mail.ru);

– Address Book (новая версия приложения для поиска информации по сотрудникам).

Наличие интеграции между ITIM и HR Access позволяет в автоматическом режиме формировать профили сотрудников в ITIM на ежедневной основе.

Если отдел кадров, создал новую карточку пользователя, то, на следующий день (синхронизация начинается примерно в 07:00) в ITIM формируется профиль пользователя с требуемым набором атрибутов.

Если отдел кадров вносит изменения в карточку пользователя в приложение HR Access, то после синхронизации эти данные попадают в ITIM.

При увольнении сотрудника, отдел кадров устанавливает дату увольнения в HR Access и эта дата, после синхронизации попадает в ITIM. Данное утверждение справедливо и для дат декретного отпуска. На основании атрибута даты увольнения в ITIM происходит блокировка профиля пользователя и всех его учетных записей, относящихся к данному профилю.

Блокировка происходит на основании процедуры (Life Cycle Rules), которая запускается ежедневно в автоматическом режиме, после синхронизации данных с HR Access.

Установлено следующее правило блокировки:

– профиль, в котором атрибут дата увольнения меньше, либо равен текущей системной дате и при этом статус профиля активен, блокируется;

– при этом, процесс настроен таким образом, что в профиле пользователя меняется адрес электронной почты – к имени почты добавляется дата блокировки. Это было сделано с целью блокировки возможности работы с почтой, если она была настроена на смартфоне пользователя.

Экстренная блокировка учётных записей производится в исключительных случаях (грубые нарушения трудовых отношений - увольнение по недоверию, подозрение в мошеннических действиях и прочее).

Блокировка учётной записи производится в ручном режиме, используя стандартную функцию ITIM для блокировки профиля.

При ручной блокировке профиля, блокируются все связанные с ним учетные записи. Меняется адрес электронной почты – к имени добавляется дата блокировки. Срок хранения заблокированных профилей в ITIM - 6 месяцев. По истечении этого срока профили удаляются, со всеми привязанными учетными записями. Процедура выполняется автоматически каждую неделю.

6.3 Разработка комплекса технических мер по ограничению и контролю доступа

Согласно проведенной комплексной оценки ИБ, в администрации города Новый Уренгой одно из основных замечаний является слабые защитные меры по ограничению доступа к сетевой инфраструктуре, особенно в помещении

серверной, и недостаточный пропускной режим, отсутствие внедрение единой системы видеонаблюдения в сеть связи и отсутствие технической системы регистрации и пропускного контроля сотрудников.

С целью устранения угрозы безопасности в администрации города Новый Уренгой планируется развернуть систему контроля и управления доступом (СКУД) на базе контроллера Орион-Про. Выбор данного оборудования продиктован тем, что в государственных учреждениях ЯНАО развернуто сетевое решение СКУД «Орион-Про», поэтому, данное решение внесено в реестр типовой инфраструктуры администраций [3].

Главное назначение СКУД - запрет на вход в помещение людей, не обладающих правом прохождения.

Составными частями СКУД являются:

– замки, турникеты, шлюзовые камеры;

– магнитные карты, электронные идентификаторы;

считывающие устройства;

– сетевые контроллеры и автономные;

– программное оборудование СКУД;

– соединительные системы позиционирования;

– оборудование для введения PIN-кода;

– камеры слежения.

СКУД «Орион-Про» также обеспечивает выполнение целого ряда вспомогательных задач, среди которых:

– приложение по учету рабочего времени;

– начисление заработной платы работникам предприятия;

– взаимодействие с системами пожаротушения и электроснабжения;

– построение графиков рабочего времени;

– контролирование работников на территории предприятия;

– резервное хранение информации о персонале.

Интегрированная система охраны «Орион» представляет собой совокупность аппаратных и программных средств, для организации систем охранно-пожарной сигнализации, контроля доступа, видеонаблюдения, автоматического пожаротушения, а также для создания систем контроля и диспетчеризации объектов [28].

Основные технические характеристики системы «Орион Про»:

– количество приборов, подключаемых к линии RS-485: до 127;

– количество зон в разделах АРМ «Орион Про»: до 16 000;

– количество разделов АРМ «Орион Про»: до 10 000;

– количество точек доступа: до 254;

– количество пользователей АРМ «Орион Про»: не ограничено.

Неоспоримым преимуществом системы СКУД «Орион-Про» является полная архитектура на основе протокола IP [28].

Архитектура СКУД «Орион-Про» представлена на рисунке 6.2 [28].

Рисунок 6.2 – Архитектура СКУД «Орион – Про»

На основе типового решения и архитектуре внедрения СКУД «Орион-Про» в ВКР спроектирована схема организации системы СКУД администрации города Новый Уренгой. Система СКУД разворачивается на основе нового коммутатора, и все остальные устройства подключаются к нему. Архитектура системы - звезда. Схема разворачивания системы представлена на рисунке 6.3.

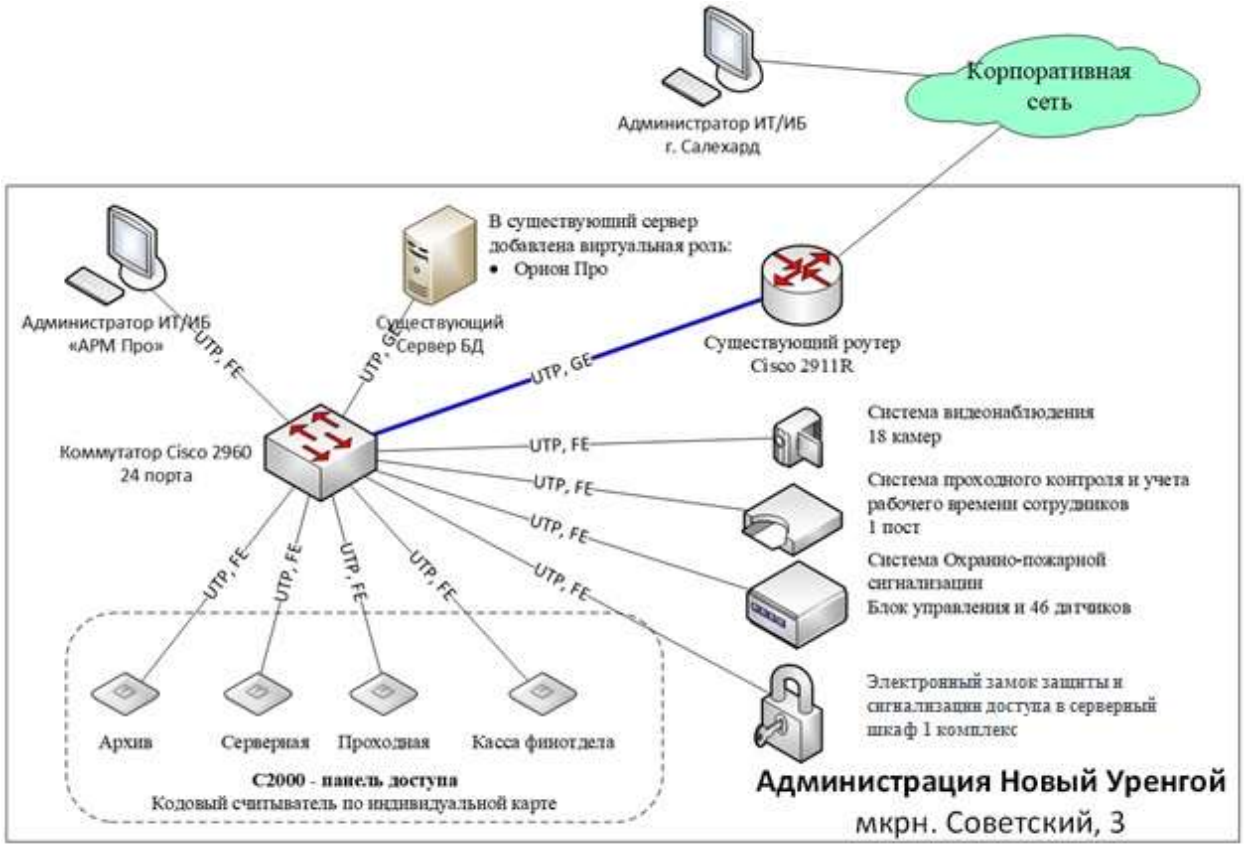

Рисунок 6.3 – Схема организации СКУД «Орион-Про»

Все функции, которые возложены на программное обеспечение СКУД «Орион-Про», обозначены в четырех группах:

– управление и мониторинг;

– расширенные возможности контроллеров;

– пропускные функции;

– дополнительные конфигурации доступа.

Разворачивание систем СКУД в администрации города Новый Уренгой включает в себя следующие виды технических установок:

– установка панелей доступа по магнитным картам;

– установление системы контроля и учета рабочего времени сотрудников;

– подключение к системе «Орион-Про» существующих систем видеонаблюдения и охранно-пожарной сигнализации;

– установка системы защиты на шкаф с телекоммуникационным и серверным оборудованием в помещении серверной.

Проектируемый комплекс ограничение доступа позволяет повысить уровень защищенности информационной и инженерной инфраструктуры администрации города Новый Уренгой.

6.4 Реорганизация локальной инфраструктуры администрации

Согласно проведенным разработанным решениям по разворачиванию системы СКУД в сетевой инфраструктуре администрации необходимо произвести небольшую реконструкцию локальной сети с частичной модернизацией.

Всего планируется выполнить:

– установить в стойку новый коммутатор Cisco 2960/24 порта, для разворачивания системы сетевой СКУД «Орион-Про»;

– обеспечить вывод управления и мониторинга системы СКУД в управление ЯНАО в городе Салехард.

Также в проекте было принято решение об установке на сервер администрации города Новый Уренгой межсетевого экран Pro Firewall, являющегося дополнительным средством защиты и фильтрации трафика. Данное решение обусловлено тем, что ПО Pro Firewall было закуплено по контракту Госторги в 2017 году управлением делами ЯНАО и декларируется к установке отдельным приказом по всем департаментам ИТ.

Разработанное схематическое решение локальной сети администрации города Новый Уренгой представлено на рисунке 6.4.

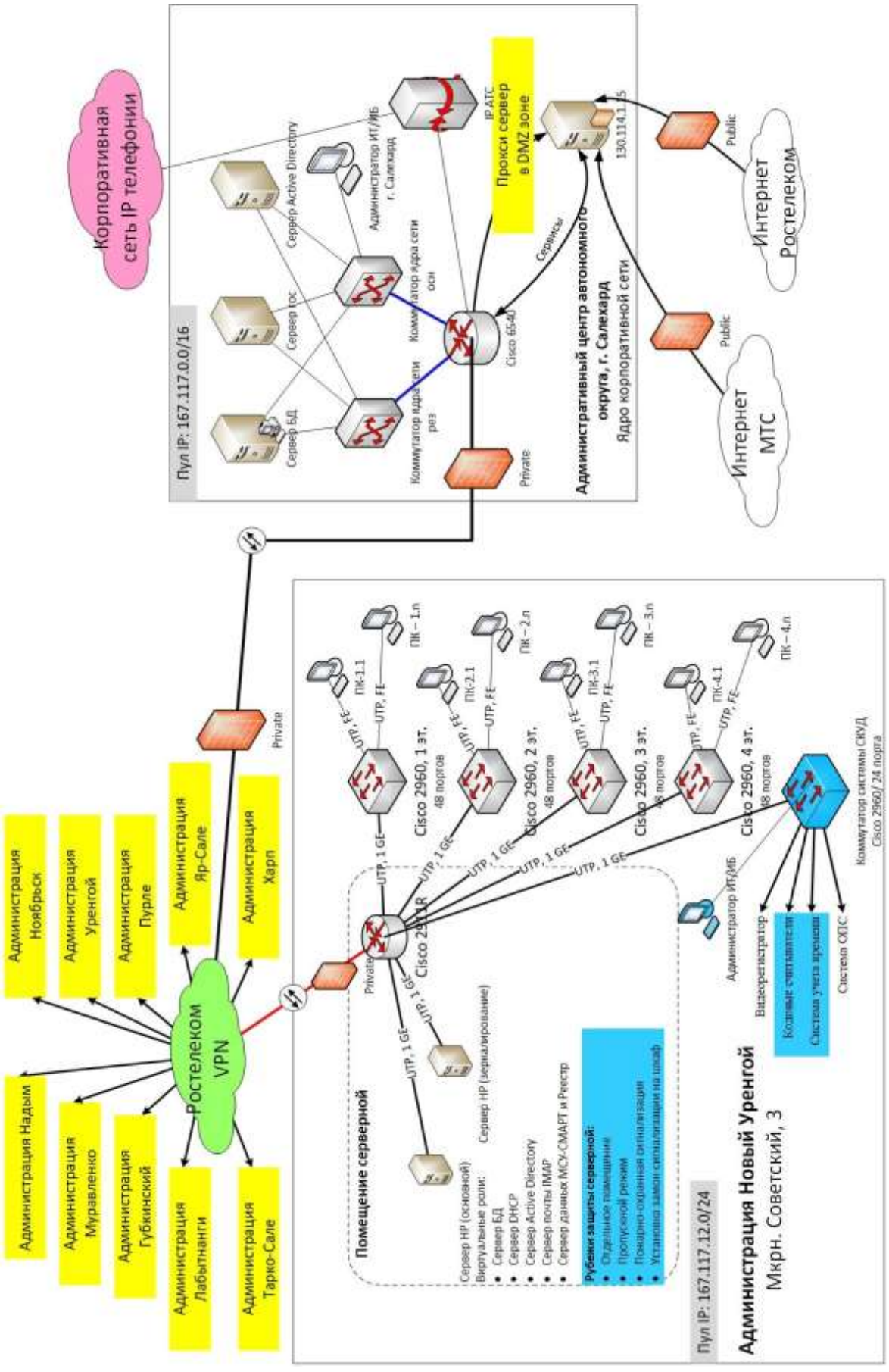
Корпоративная сеть IP телефонии
Пул IP: 157.117.0.0/16
Сервер Active Directory
Сервер tos
Сервер БД
Коммутатор ядра сети
Коммутатор ядра сети
Администратор ИТ/ИБ г. Салехард
IP АТС
Прокси сервер в DMZ зоне
Cisco 6540
Private
Сервисы
130.114.1.15
Public
Public
Административный центр автономного округа, г. Салехард
Ядро корпоративной сети
Интернет Ростелеком
Интернет МТС
Ростелеком VPN
Private
Администрация Ноябрьск
Администрация Урентой
Администрация Пурпе
Администрация Яр-Сале
Администрация Харп
Администрация Надым
Администрация Муравленко
Администрация Губкинский
Администрация Лабытнанги
Администрация Тарко-Сале
Помещение серверной
Cisco 2811 R
Private
Сервер HP (основной)
Виртуальные роли:
Сервер БД
Сервер DHCP
Сервер Active Directory
Сервер почты IMAP
Сервер данных МСУ-СМАРТ и Реестр
Сервер HP (зеркалирование)
Рубежи защиты серверной:
Отдельное помещение
Пропускной режим
Пожарно-охранная сигнализация
Установка замки-сигнализации на шкаф
Пул IP: 167.117.12.0/24
Администрация Новый Уренгой
Мкрн. Советский, 3
Cisco 2960, 1 эт. 48 портов
Cisco 2960, 2 эт. 48 портов
Cisco 2960, 3 эт. 48 портов
Cisco 2960, 4 эт. 48 портов
ПК-1.1
ПК-1.n
ПК-2.1
ПК-2.n
ПК-3.1
ПК-3.n
ПК-4.1
ПК-4.n
UTP, FE
UTP, 1 GE
Администратор ИТ/ИБ
Видеорегистратор
Копные считыватели
Система учета времени
Система ОДС
Коммутатор системы СКУД Cisco 2960/ 24 порта

Рисунок 6.4

6.5 Выбор отраслевого решения информационной безопасности

Обеспечение безопасности важных государственных проектов и персональных данных граждан страны – основной приоритет для создания качественной IT государственных организаций.

Основной задачей повышение информационной безопасности администрации города Новый Уренгой является устранения угрозы социальной инженерии. В проекте планируется определить специализированное программное обеспечение, позволяющее проводить мониторинг и учет действий в общей информационной инфраструктуре администрации.

Для администрации города Новый Уренгой планируется изучить и внедрить отраслевое решение компании InfoWatch по обеспечению информационной безопасности государственных учреждений. Решения данной компании сертифицированы в ФСБ и ФСТЭК и рекомендованы для внедрения в учреждениях госсектора.

Решение компании InfoWatch применяются на всех объектах муниципальных образований ЯНАО, так как компания выиграла тендер на разработку и поставку специализированного ПО, для нужд администраций в 2016 году.

Помимо решений компании InfoWatch в тендере рассматривались программы:

– Securit ZGate;

– Symantec Data Loss Prevention;

– Search Inform Контур безопасности;

– FalconGaze SecureTower.

Сравнительный анализ сравнения предложенных решений приведен в таблице 6.1.

Таблица 6.1 – Сравнительный анализ решений по предотвращению утечек

Показатель	SecurIT	InfoWatch	Symantec	SearchInform	FalconGaze
Название системы	ZGate	TrafficMonitor	DataLossPrevention	Контур безопасности	SecureTower
Модульность системы	Да	Нет	Нет	Да	Нет
Роли	Любое количество	Несколько	Любое количество	Любое количество	Администратор системы ИБ

Продолжение таблицы 6.1

Места установки	На сервер+ZLock на клиентские ПК	Сервер, клиент	Сервер, клиент	Сервер, клиент	Сервер, клиент
Лицензирование	Почтовые ящики, рабочие места	Каналы перехвата, технологии анализа	n/a	Сервер, mail, IM, Skype, Print, device, HTTP, FTP	Рабочее место
Контроль IM	Да	Да	Да	Да	Да
Наличие сертификатов и лицензий	ФСТЭК НДВ 3 и ОУД4	ФСТЭК НДВ 4 и ИСПДн 1, Газпромсерт, Аккредитация ЦБ, сертификат совместимости eToken	ФСТЭК НДВ 4	ФСТЭК НДВ 4	ФСТЭК НДВ 4 и ИСПДн 2
Контроль HTTP/HTTPS, FTP	Да	Да	Да	Да	Да
Контроль Skype	Текст	Текст	Нет	Да	Да
Контроль E-mail	Да	Да	Да	Да	Да
Социальные сети и блоги	Да	Да	Да	Да	Да
Контроль подключаемых внешних устройств	При покупке Zlock	Да	Да	Да	Нет
Блокируемые протоколы	HTTP, HTTPS, SMTP, OSCAR	HTTP, HTTPS, FTP, FTP over HTTP, FTPS, SMTP, SMTP/S, ESMTP, POP3, POP3S,	SMTP, HTTP, HTTPS FTP, Yahoo Messenger, MSN Messenger, AIM, AIM Pro Messenger,	SMTP, POP3, MAPI, IMAP, HTTP,FTP, ICQ, Jabber	HTTP, HTTPS, FTP, FTTPS, Вся почта и IM

		IMAP4, IMAP4S	MSN Messenger, AIM		
Лингвистический анализ	Да	Да+БКФ	Нет	да	Да
Анализ транслита	Да	Да	Нет	n/a	n/a
Анализ по словарю	Да	Да	Да	Да	Да
Анализ архивов	Да	Да	Да	Да	Да
Контроль портов	USB,COM,LPT, Wi-Fi	USB,COM,LPT, Wi-Fi, Bluetoot	USB,COM,LPT, Wi-Fi, Bluetooth	USB, LPT	USB, LPT
Анализ рисунков	Да	Да	Да	Да	Нет
Предустановленные шаблоны фильтрации	Да	Да	Да	Да	Да
Задержка отправки подозрительных сообщений	Да, ОБ принимает решение	Да, ОБ принимает решение	Да, пользователь объясняет причину отправки, инцидент фиксируется	n/a	Нет, только информирование офицера ИБ
Режим установки агентов	Открытый	n/a	n/a	n/a	Тайный/Открытый
Защита агентов от выключения	Да	Да	Да	Да	Да
Запись отчетов в локальное хранилище в случае недоступности сервера	Да	Да	Да	Да	Да

Просмотр истории инцедентов	Да	Да	Да	Да	Да
Возможность тестирования продукта на серверах разработчика	нет	нет	Да	нет	на сервере дистрибьютора
Возможность получения демо-версии для тестирования внутри организации	±	±	нет	±	Да, 1 месяц
Режимы оповещений	Консоль, почта, графики	Консоль, почта	Консоль, почта, графики	Консоль, почта, графики	Консоль, почта, графики
Логирование действий администраторов системы	Да	Да	Да	n/a	В случае утановки агента на РМ администратора

Показатель	SecurIT	InfoWatch	Symantec	SearchInform	FalconGaze
Цена для компании 250 ПК, тыс. руб.	2500	105	457	3300-4500	150

На основании проведенного анализа в ходе проведения Госторгов выиграли решения компании InfoWatch, так как обладают хорошей функциональностью, сертификации ФСБ и низкой стоимостью продукта.

Компания InfoWatch - российский разработчик и поставщик программного обеспечения, обладающий всеми необходимыми лицензиями и сертификатами ФСТЭК, ФСБ, систем добровольной сертификации. Компания InfoWatch входит в ассоциацию разработчиков программных продуктов «Отечественный Софт».

Для целей повышения эффективности и имиджа администрации города Новый Уренгой, выбраны два программных решения наиболее полно отражающих специфику дел [29]:

– Infowatch Endpoint Security;

– Infowatch Kribrum.

Объекты защиты в сфере государственного сектора [29]:

– государственная тайна;

– коммерческая тайна (данные договоров с партнерами и подрядчиками, данные конкурсных процедур);

– персональные данные;

– веб-ресурсы учреждения (доступность веб-портала);

– репутация учреждения.

Решения Infowatch позволяют:

– защитить критически важную информацию и персональные данные клиентов;

– защитить бизнес-процессы, связанные с обработкой конфиденциальных данных;

– выявить нелояльных сотрудников и злоумышленников, сговоры;

– снизить репутационные риски, связанные с возможными утечками информации в социальных сетях;

– предотвратить атаки на веб-ресурсы;

– соответствовать требованиям регуляторов.

Решение InfoWatch Traffic Monitor Enterprise помогает государственным органам соответствовать требованиям

– федерального закона №152-ФЗ «О персональных данных»;

– федерального закона №273-ФЗ «О противодействии коррупции»;

– постановления Правительства РФ №1119 «Об утверждении требований к защите ПДн при обработке в информационных системах ПДн»;

– приказа №21 ФСТЭК России.

Спецификация и назначение решений в госсекторе:

1) Infowatch Traffic Monitor

Программное решение (DLP-система), предназначенное для контроля информационных потоков, защиты конфиденциальной информации от утечки и несанкционированного распространения.

Предотвращает внутренние угрозы и нарушения, ведущие к финансовым потерям. Выявляет сговоры кредитных специалистов с клиентами, попытки кражи номеров банковских карт и баз данных, фальсификацию кредитных договоров.

2) Infowatch Attack Killer

Защищает от внешних атак веб-ресурсы компании. Обеспечивает доступность веб-ресурсов, порталов и заполняемых форм обратной связи.

Комплексная активная автоматизированная защита веб-приложений от хакерских взломов и DDoS-атак.

3) Infowatch Endpoint Security

Выявляет нелояльных сотрудников и бездельников. Осуществляет мониторинг рабочей активности сотрудников, проводит детальный аудит использования инфраструктуры компании.

Программный продукт для обеспечения безопасности информации на рабочих станциях, съемных носителях и мобильных устройствах, ориентированный на оперативное развертывание и простоту управления.

4) Infowatch Kribrum

Собирает упоминания объекта (компания, персона, продукт компании) из русскоязычных ресурсов Интернета: социальных сетей, онлайн-СМИ, блогов, форумов и других ресурсов.

6.6 Разворачивание система Infowatch Endpoint Security

Для обеспечения безопасности и разворачивания контроля за операционной деятельностью сотрудников, в администрации города Новый Уренгой планируется развернуть отраслевую систему Infowatch Endpoint Security.

Разворачивание системы Infowatch Endpoint Security разделено на несколько этапов, как представлено ниже.

1) Подготовительный этап:

– заполнение опросного листа;

– подписание юридических договоров;

– согласование старта и времени проведения пилота;

– определение мощностей для развёртывания;

– продолжительность этапа от 2х до 5 дней.

2) Этап внедрения:

– подготовка серверов;

– развёртывание систем;

– интеграция в инфраструктуру заказчика;

– распространение клиентов на рабочие станции;

– продолжительность этапа от 1 до 3х дней.

3) Тестирование:

– проверка корректности работы системы;

– инструктаж по работе с системой;

– ответы на возникающие вопросы;

– тестирование самого продукта;

– продолжительность этапа от 3х до 8 недель.

4) Подведение Итогов

– подведение итогов;

– привлечение аналитика из компании InfoWatch для составления отчёта;

– вывод всех систем из инфраструктуры администрации;

– продолжительность этапа от 3х до 8 дней.

Назначение системы Infowatch Endpoint Security:

– защита бизнеса от финансовых потерь и нерационального использования рабочего времени;

– детализированный аудит поведения персонала и использования инфраструктуры компании;

– мониторинг рабочей активности сотрудников.

Ключевые возможности:

– автоматический мониторинг и диагностика слабых мест в ИТ-инфраструктуре и работе персонала;

– управление запуском приложений;

– быстрое и надежное шифрование данных;

– контроль доступа сотрудников к внешним устройствам и файлам;

– мгновенное удаление данных на ПК и мобильных устройствах;

– безопасная работа в облачных хранилищах;

– централизованные политики безопасности для мобильных устройств;

– green IT.

Сертификация системы:

– сертифицировано ФСТЭК России;

– сертификат ФСТЭК №3306 от 23 декабря 2014 г.;

Подтверждает соответствие InfoWatch EndPoint Security 4 уровню контроля отсутствия НДВ и дает возможность применять InfoWatch EndPoint Security в информационных системах персональных данных всех уровней защищенности, а также в государственных, финансовых, промышленных и других организациях, где требуются использование сертифицированного ПО.

Система InfoWatch EndPoint Security Insight Edition реализует концепцию «сначала понять ситуацию, затем выстроить систему защиты».

Рисунок 6.5 – Архитектура системы

Модуль Insight установленный в администрации собирает данные [29]:

1) На уровне периферии:

– копирование данных на внешние устройства: кто, когда, какую информацию записывает на съемные носители;

– использование внешних устройств и съемных носителей;

– назначенные на сотрудников права доступа к файлам и внешним устройствам;

– анализ активности персонала по рабочим часам и дням;

– категории данных, копируемых сотрудниками (exe-файлы, документы, xls-файлы, видеофайлы, логи и т.д.), на внешние носители;

– попытки доступа к запрещенным устройствам и файлам.

2) На уровне сетевых каталогов:

– наиболее популярные классы устройств (сетевые папки, облачные хранилища, терминальные диски);

– статистика использования сотрудниками и отделами использования сетевых каталогов;

– анализ активности персонала по рабочим часам и дням;

– категории данных, копируемых сотрудниками в сетевые каталоги (exe-файлы, документы, xls-файлы, видеофайлы, логи и т.д.).

3) На уровне приложений:

– статистика запуска и использования приложений;

– наиболее популярные приложения конкретного сотрудника или отдела;

– фоновая и активная работа приложений на компьютерах сотрудников;

– категорирование приложений (например, рабочие и нерабочие приложения);

– возможность удаления программы или приложения прямо в консоли.

4) На уровне сети интернет:

– посещение сотрудниками различных категорий сайтов;

– активность сотрудников в сети Интернет по рабочим часам или дням;

– статистика фонового и активного использования Интернет-ресурсов.

Система защиты Infowatch Endpoint Security:

5) Разграничение доступа сотрудников к важной информации

В процессе работы сотрудники администрации активно пользуются съемными носителями, флешками и другими коммуникационными устройствами – всё это несет серьезный риск того, что сотрудники скопируют и используют в личных целях важную информацию.

InfoWatch EndPoint Security обеспечивает контроль доступа к устройствам, портам, сетевым интерфейсам, сетевым каталогам и облачным хранилищам. Продукт предлагает множество возможностей для управления правами доступа [29]:

– по списку разрешенных классов носителей;

– по разрешенным моделям устройств;

– по серийному номеру устройства;

– по списку разрешенных беспроводных сетей.

6) Контроль информации во время ее копирования, хранения и использования в облачных хранилищах

InfoWatch EndPoint Security отслеживает все файлы, отправляемые сотрудниками в Dropbox, SkyDrive, GoogleDrive, ЯндексДиск, BoxSync, а также регулирует эти процессы, запрещая или разрешая перемещение документов по определенному типу и формату данных.

7) Защита информации от кражи при потере ноутбуков и флешек

Съемные носители и ноутбуки – наиболее уязвимое звено в корпоративной инфраструктуре компании, поскольку сотрудники их часто теряют или «забывают».

InfoWatch EndPoint Security предлагает простой и удобный способ защитить информацию, зашифровав данные:

– никто из посторонних людей не сможет прочитать данные;

– все данные автоматически шифруются сразу при их создании, не мешая сотрудникам и не требуя дополнительных временных затрат (прозрачное шифрование).

Продукт может шифровать информацию на ноутбуках, ПК, внешних устройствах, каталогах облачных хранилищ.

Шифрование данных происходит в фоновом режиме и абсолютно прозрачно незаметно для сотрудников.

8) Система отчетов

Отчеты позволяют просматривать журналы событий, назначения и изменения прав пользователей, активности компьютеров, состояние системы.

Система выстроена по принципу мониторинг – действие. Данная функция выполняется модулем Insight, который является агрегатором событий. Собранная с помощью Insight статистика служит основанием формирования наглядных отчетов, которые дают целостное представление о ситуации в компании и детальную информацию о работе конкретных сотрудников либо отделов.

Окно аудита программы Insight изображено на рисунке 6.6.

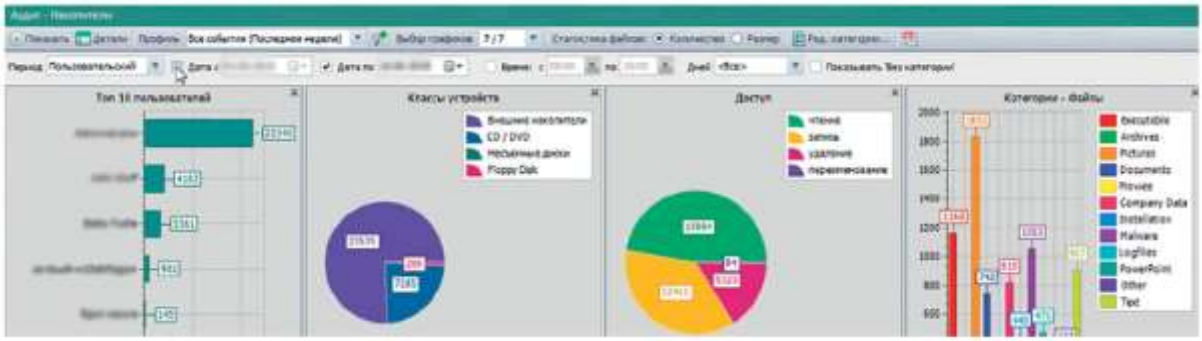

Рисунок 6.6 – Аудит модуль системы Insight

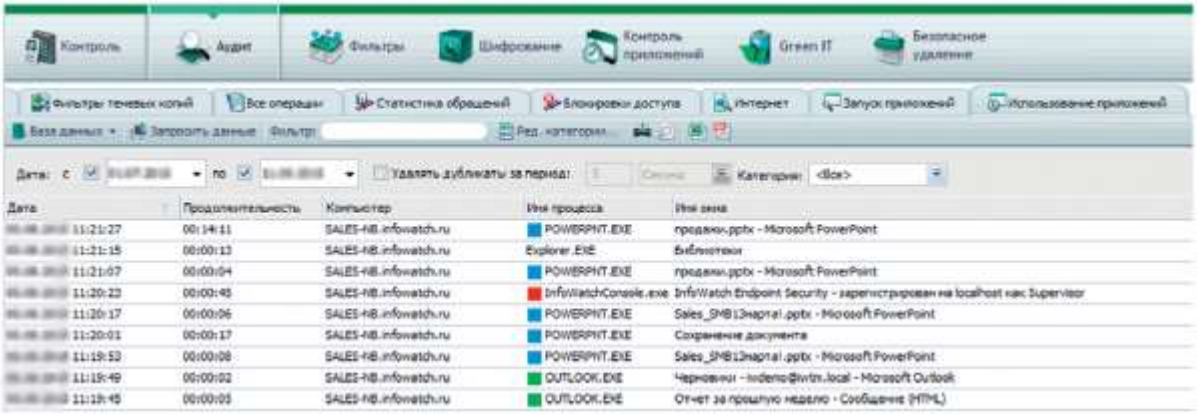

Рисунок 6.7 – Фильтр операций системы

Аудит обеспечивает контроль доступа сотрудников к приложениям с помощью «белого» и «черного» списков. Это гарантирует, что любая программа или приложение, не связанные с работой, не будут установлены или запущены на компьютере администрации.

InfoWatch EndPoint Security обеспечивает контроль доступа к устройствам, портам, сетевым интерфейсам, сетевым каталогам и облачным хранилищам. Продукт контролирует более 20 видов различных устройств.

Рисунок 6.8 – Шифрование данных в системе

Гибкие настройки шифрования ориентированы на решение различных бизнес-задач: можно настроить доступ к зашифрованным файлам для всех сотрудников компании, группе пользователей (например, сотрудникам отдела) или только одному сотруднику [29].

Основное предназначение системы для государственных организаций - это расширенные возможности инсайд. Окно слежение за деятельностью организации представлено на рисунке 6.9.

Рисунок 6.9 – Окно слежения за деятельностью сотрудников и ПО

Возможности модуля Insight:

– отображение событий в режиме реального времени для обнаружения угроз и возможных слабых мест, что позволяет увидеть полную картину ситуации в компании;

– создание подробных отчетов по доступу к данным и действиям;

– получение оперативной информации об активности сотрудников в течение рабочего дня;

– обоснование для принятия взвешенных решений относительно оптимизации работы персонала и контроля ИТ-инфраструктуры.

Выводы по разделу шесть

Система Insight выставлена на конкурсной основе на площадку Госторги, с целью приобретения и внедрения силами департамента информационной инфраструктуры администрации города Новый Уренгой.

Данная система позволяет полностью контролировать информационные потоки, занятость сотрудников и типы задействованного ПО.

Таким образом, внедренная система позволяет контролировать исполнение всех должностных инструкций и противостоять противоправным и неэффективным действиям.

Каждый сотрудник будет письменно уведомлен о внедрении системы, о ее возможностях и функциях, что напрямую послужит стимуляцией более оперативно и качественно выполнять свою работу.

Разработанный комплекс технических мер позволит поднять уровень функциональности информационной сети на новый уровень и кардинально изменить информационную и структурную администрации города Новый Уренгой.

7 ПОСТПРОЕКТНЫЙ АУДИТ ПОСЛЕ ПРИНЯТИЯ КОМПЛЕКСА МЕР

7.1 Постановка задачи

В данной главе планируется произвести постпроектный аудит ИБ после принятия комплексных мер, произвести постпроектный анализ ИБ администрации системой MSAT, произвести поспроектную проверку информационной безопасности информационными листами.

7.2 Постпроектный анализ ИБ администрации системой MSAT

В данном разделе ВКР проводится постпроектный анализ уровня информационной защищенности и информационной безопасности администрации города Новый Уренгой после проведения комплекса организационных и технических мер. Постпроектный анализ информационной защищённости, произведенный системой MSAT производится с целью качественного определения повышения информационной защищенности администрации [11].

Результат отчета, полученный в ходе постпроектной оценки ИБ представлен на рисунке 7.1.

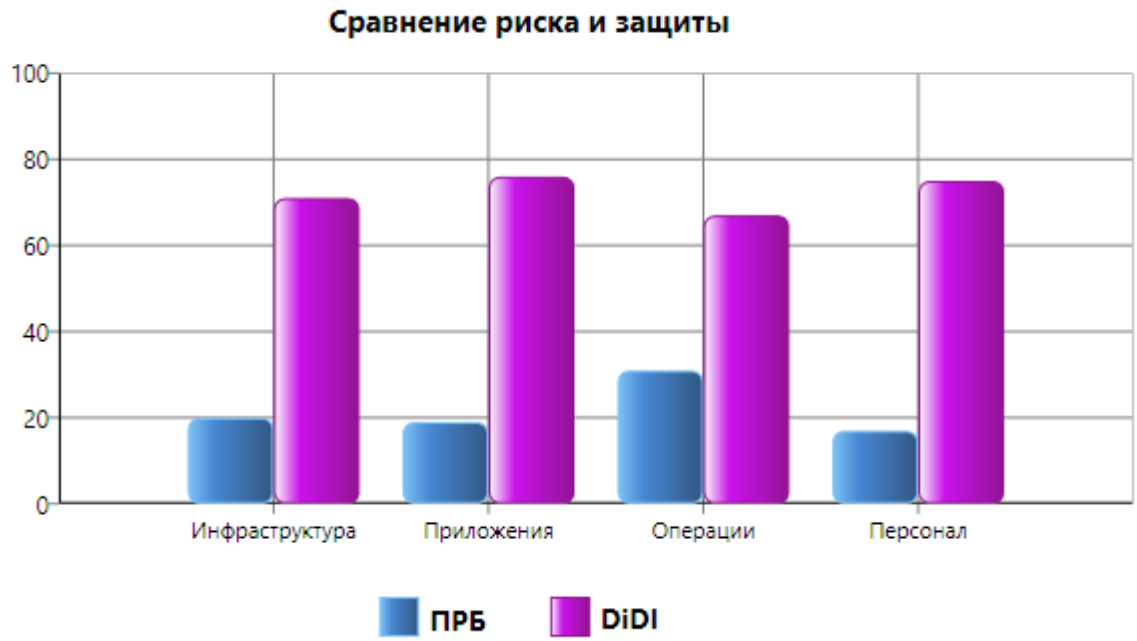

Рисунок 7.1 – Построектный отчет анализа информационной безопасности

Подводя итог постпроектной оценки ИБ получены следующие процентные изменения по показателям:

– инфраструктура: 22 %;

– приложения: 26 %;

– операции: 43 %;

– персонал: 51 %.

Показатель ПРБ находится в диапазоне от 15 до 30, тем самым показатель потенциального риска для бизнеса в данной специфической области анализа небольшой и после внедрения защитных мер, его значение кардинально уменьшилось. Нулевое значение в принципе невозможно, так как деловая деятельность сама по себе подразумевает наличие какого-то уровня риска. Кроме того, важно понимать, что существуют определенные аспекты ведения бизнеса, для которых отсутствует прямая стратегия снижения риска.

Показатель DiDI после принятия мер существенно вырос. Это говорит о том, что принятые меры принесли результат, в администрации города Новый Уренгой принято множество мер для развертывания стратегий эшелонированной защиты (DiD) в областях инфраструктуры, приложений, операций и персонала. Стоит уточнить, что показатель DiDI не отражает общей эффективности безопасности или же ресурсы, затраченные на безопасность.

Полученные низкие значения показателя ПРБ и высокие значения показателя DiDI, означают что, принятые меры значительно повышают защищенность и информационную безопасность администрации города Новый Уренгой.

7.3 Поспроектная оценка ИБ опросными листами

В данной главе ВКР проведена постпроектная оценка уровня защищенности и информационной безопасности по опросным листам, разработанным в главе 2.

Программа основана на списке вопросов и значениях коэффициентов значимости этих вопросов. Согласно проведенной оценки исходных условий была получена оценка информационной безопасности, которая оказалась довольно низкой за счет недостаточности защищенности помещения серверной и физических сетей, а также беспроводной сети предприятия.

После проведения организационно-правовых и технических мер, направленных на устранение недостатков и пробелов в системе защиты, в ВКР проведена повторная оценка с целью выяснения эффективности проектных решений.

Итоговые оценки всех критериев постпроектного состояния администрации города Новый Уренгой, сформированы в итоговой таблице в отдельном разделе программы, в которой происходит объединение критериев в логические группы и

вывод итоговой оценки соответствия ИБ организации. Результаты оценки итоговой таблицы представлены в приложении В.

Согласно проведенного, оценки соответствия после принятия мер направленных на повышение защищенности, программа выдала значение оценки: 0,85.

Согласно проведенным предпроектным и постпроектным оценкам ИБ администрации города Новый Уренгой, после принятия комплекса мер получено, что значение комплексной оценки повысилось на 0,44 пункта. Данный показатель свидетельствует об эффективности принятия мер по защите инфраструктуры администрации города Новый Уренгой.

Итоговое значение можно интерпретировать как «очень высокое», поскольку все слабые места ликвидированы, а внедренные защитные меры значительно повысили уровень информационной безопасности администрации города Новый Уренгой. Защите оборудования, линий связи, учета деятельности сотрудников и мониторинга их активности, а также вопросам доступа в серверное помещение уделено особое внимание.

ЗАКЛЮЧЕНИЕ

Целью выполнения ВКР является разработка мер по повышению уровня защищенности и информационной безопасности администрации города Новый Уренгой.

В ходе проведения работы над ВКР произведен анализ и сбор исходных данных об объекте проектирования, рассмотрена организационная структура, сетевая и информационная инфраструктура. На основании собранной информации принято решение о проведение проектных работ, направленных на повышение уровня защищенности.

Точкой старта работ над проектированием началось с исходного анализа информационной защищенности администрации города Новый Уренгой посредством комплекса MSAT а так же разработана собственная система опросных листов по оценке информационной безопасности и произведена апробация в администрации. Полученный сводный отчет показал недостаточное значение защищенности. Согласно отчету определены точки и критерии безопасности которым уделено слабое внимание. Анализ системы MSAT также показал основные виды информационных угроз и выявление каналов утечки информации, которые могут произойти в администрации.

Согласно полученной оценки слабыми местами в администрации города Новый Уренгой оказались системы связи, защищенность серверной и недостаточный контроль за действиями сотрудников администрации, представляющих большую угрозу утечки информации по принципу социальной инженерии.

Следующим шагом в ВКР произведен комплекс мер по повышению уровня защищенности информационной безопасности в организационной сфере. Принятые меры относятся к планированию информационной защищенности и повышения квалификации администратора ИБ, с целью получения необходимых знаний и навыков.

Далее в ВКР проведен комплекс организационных и технических мер направленный на повышение защищенности администрации города Новый Уренгой.

Технический радел заканчивается проектом модернизации локальной сети администрации города Новый Уренгой, установкой дополнительного коммутатора для нужд системы СКУД, выделение на сервере новой виртуальной роли для системы СКУД. Отдельно рассмотрено внедрение системы Infowatch Endpoint Security. Позволяющим вести контроль за операционной деятельность

сотрудников и производимых ими действий в базе данных и программном обеспечении администрации.

Завершающим этапом проектных мер является построенная оценка уровня информационной безопасности и общей защищенности. Согласно проведенной оценке системой MSAT удалось повысить следующие показатели:

– инфраструктура: 22 %;

– приложения: 26 %;

– операции: 43 %;

– персонал: 51 %.

Проведение оценки по разработанным опросным листам показало значение постпроектной защищенности 0,85 пунктов, что на 0,44 пункта выше начального результата.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Галатенко, В.А. Стандарты информационной безопасности. М.: Интернет-университет информационных технологий, 2010. - 264 с.

2 Ярочкин, В.И. Информационная безопасность. Учебник для студентов вузов // 3-е изд. - М.: В.И. Ярочкин, 2012г. - 544 с.

3 Сайт администрации город Новый Уренгой URL: http://www.newurengoy.ru [Электронный ресурс] (дата обращения: 1.01.2018 г.)

4 Компания КейСистемс URL: https://www.keysystems.ru/products/MunSelfSMART/ [Электронный ресурс] (дата обращения: 12.03.2018 г.)

5 Система Госуслуг URL: http://fileregionuc.nso.ru/Wiki/ [Электронный ресурс] (дата обращения: 12.03.2018 г.)

6 Сайт компании Cisco URL: www.cisco.com [Электронный ресурс] (дата обращения: 1.04.2018 г.)

7 Парфенов Н. П., Стахно Р. Е. Технология защиты персональных данных//Наука, техника и образование, 2016. № 4 (22)

8 Домбровская Л. А., Васютина Т. Л. Организационные средства защиты информации как элемент общей системы защиты информации//EUROPEAN SCIENCE, 2016. № 11 (21)

9 Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: Учебник для вузов / ООО «Издательство Машиностроение», 2009 – 508 с

10 Шаньгин, В.Ф. Комплексная информация в корпоративных системах: учеб. пособие. – М.: ИД «Форум», «ИНФРА- М», 2010 – 592 с.

11 Сайт системы MSAT: https://technet.microsoft.com/ru-ru/security/cc15712.aspx [Электронный ресурс] (дата обращения: 1.1.2018 г.)

12 Базовая модель гроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка), федеральная служба по техническому и экспортному контролю, утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

13 Киселев А.А. Методические указания к выполнению курсовой работы по дисциплине «Методология оценки безопасности информационных технологий» для студентов заочного обучения, профиль «Защищенные системы и сети связи» Новосибирск, 2014. – 20 с.

14 ГОСТ Р-27001-2006 Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности.

Требования. URL: http://docs.cntd.ru/document/1200058325 (дата обращения: 5.04.2018 г.)

15 ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. URL: http://www.consultant.ru/cons/cgi/online.cgi (дата обращения 5.04.2018 г.)

16 ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. URL: http://docs.cntd.ru/document/1200084141/ (дата обращения 5.04.2018 г.)

17 ГОСТ Р МЭК 61508-3-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных связанных с безопасностью. Часть 3. Требования к программному обеспечению. URL: http://docs.cntd.ru/document/1200100350 (дата обращения 5.04.2018 г.)

18 ГОСТ Р ИСО/МЭК ТО 19791-2008 Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. URL: http://docs.cntd.ru/document/1200076806/ (дата обращения 5.04.2018 г.)

19 ГОСТ Р ИСО/МЭК 27002-2012 Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности в организациях. URL: http://docs.cntd.ru/document/1200103619/ (дата обращения 1.01.2018 г.)

20 ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования. URL: http://docs.cntd.ru/document/1200113802/ (дата обращения 7.04.2018 г.)

21 ГОСТ Р 18044-2007 Менеджмент инцидентов информационной безопасности. URL: http://docs.cntd.ru/document/1200068822 (дата обращения 7.04.2018 г.)

22 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: http://docs.cntd.ru/document/1200068741 (дата обращения 7.04.2018 г.)

23 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». URL: http://docs.cntd.ru/document/1200061496 (дата обращения 7.04.2018 г.)

24 Нормативно-методический документ ФСТЭК России от 15.02.2008 «Об утверждении Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных». URL: http://docs.cntd.ru/document/1200066521 (дата обращения 15.04.2018 г.)

25 Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие для студ. высш. учеб. заведений. – М.: Издательский центр «Академия», 2008 – 336 с.

26 Учебный центр специалист URL: http://www.specialist.ru/information-security [Электронный ресурс] (дата обращения: 15.04.2018 г.)

27 Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности». URL: http://docs.cntd.ru/document/12054061496 (дата обращения 1.01.2018 г.)

28 Сайт компании интегратора систем безопасности Грумант URL: https://www.grumant.ru/prices/retail/673/ [Электронный ресурс] (дата обращения: 1.01.2018 г.)

29 Группа компаний infowatch URL: https://www.infowatch.ru [Электронный ресурс] (дата обращения: 15.04.2018 г.)

30 Галицкий, А.В., Защита информации в сети - анализ технологий и синтез решений. Рябко С.Д., Шаньгин В.Ф.- М.: ДМК Пресс, 2011. - 616 с.

31 Сайт компании Нод 32 URL: https://www.esetnod32.ru [Электронный ресурс] (дата обращения: 19.03.2018 г.)

32 Федеральный закон "О безопасности" от 28.12.2010 N 390-ФЗ (действующая редакция, 2016) URL: http://www.consultant.ru/document/cons_108546/ (дата обращения 12.03.2018 г.)

Приложение Б – Результаты предпроектного анализа ИБ

М1 – Система менеджмента ИБ															
№ вопр.	Вопрос к критерию	Ответ на вопрос в вероятностной форме												Коэф. Значимости (из главы 2.4)	Перенормированный коэффициент значимости	Вычисленное значение
		0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	Н/О			
1	Обозначены ли требования к разработке СУИБ?											1		0,3	0,35	0,35
2	Осуществляется ли постоянный контроль за выполнением требований ИБ?						1							0,2	0,24	0,12
3	Определена ли ответственности сотрудников администрации за невыполнение требований ИБ?				1									0,1	0,12	0,04
4	Предусмотрен ли аудит СУИБ?						1							0,05	0,06	0,03
5	Предусмотрено ли постоянное улучшение организации СУИБ?												1	0,1	0,00	0,00
6	Прописаны ли требования к ведению документации ИБ?			1										0,2	0,24	0,05
7	Защищены ли результаты аудита от внешнего доступа к ним?												1	0,05	0,00	0,00
Итоговая оценка критерия:																0,58

Рисунок Б.1 - Таблица для ввода ответов на вопросы критерия М1 и вывод значения оценки соответствия критерия

М2 - Защита персональных данных граждан (контрагентов)																
№ вопр.	Вопрос к критерию	Ответ на вопрос в вероятностной форме												Коэф. Значимости (из главы 2.4)	Перенормированный коэффициент значимости	Вычисленное значение
		0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	Н/О			
1	Прописан ли регламент обработки ПДн?											1		0,2	0,24	0,24
2	Соблюдение требований обеспечения ИБ ПДн?											1		0,3	0,35	0,35
3	Осуществляется ли контроль за сотрудниками ответственными за защиту ПДн?												1	0,1	0,00	0,00
4	Прописаны ли правила архивного хранения ПДн?												1	0,05	0,00	0,00
5	Считается ли нарушение режима защиты ПДн грубым проступком и приводит к дисциплинарной ответственности?											1		0,1	0,12	0,12
6	Гарантирована ли конфиденциальность ПД на всех этапах обработки ПД?			1										0,15	0,18	0,04
7	Формируется ли перечень документов, содержащих ПД?						1							0,1	0,12	0,06
Итоговая оценка критерия:																0,80

Рисунок Б.2 - Таблица для ввода ответов на вопросы критерия М2 и вывод значения оценки соответствия критерия

М3 - Управление доступом																
№ вопр.	Вопрос к критерию	Ответ на вопрос в вероятностной форме												Коэф. Значимости (из главы 2.4)	Перенормированный коэффициент значимости	Вычисленное значение
		0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	Н/О			
1	Рассматриваются ли уровни доступа к ИСПД?	1												0,1	0,11	0,00
2	Приняты ли меры по ограничению доступа посторонних лиц к ИСПД?						1							0,3	0,32	0,16
3	Осуществляется ли контроль за соблюдение режима доступности?											1		0,2	0,21	0,21
4	Предусмотрена ли автоматизированная система ограничения доступа?					1								0,05	0,05	0,02
5	Внедрена ли политика ограничения доступа к к ИСПД?						1							0,1	0,11	0,05
6	Предусмотрена ли ответственность за нарушение режима доступа к ИСДП?				1									0,2	0,21	0,06
7	Регламентируются ли порядок расследования нарушения контроля доступа?												1	0,05	0,00	0,00
Итоговая оценка критерия:																0,51

Рисунок Б.3 - Таблица для ввода ответов на вопросы критерия М3 и вывод значения оценки соответствия критерия

М4 - Физическая безопасность															
№ вопр.	Вопрос к критерию	Ответ на вопрос в вероятностной форме												Коэф. Значимости (из главы 2.4)	Перенормированный коэффициент значимости	Вычисленное значение
		0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	Н/О			
1	Степень защищенности материальных фондов?						1							0,3	0,32	0,16
2	Регламентируется ли специальная проверка компонентов СКУД?				1									0,1	0,11	0,03
3	Предусмотрены ли меры по препятствию вторжения в системы связи (закладки, сканирование диапазона)?			1										0,3	0,32	0,06
4	Предусмотрена ли система о предупреждении о атаке?												1	0,05	0,00	0,00
5	Обозначены ли функциональные требования к защите технических систем?											1		0,1	0,11	0,11
6	Рассматриваются ли требования экономической целесообразности к защите технических систем?											1		0,05	0,05	0,05
7	Разработана ли инструкция по мерам противодействия злоумышленникам?	1												0,1	0,11	0,00
Итоговая оценка критерия:																0,41

Рисунок Б.4 - Таблица для ввода ответов на вопросы критерия М4 и вывод значения оценки соответствия критерия

М5 – Безопасность, связанная с сотрудниками															
№ вопр.	Вопрос к критерию	Ответ на вопрос в вероятностной форме												Коэф. Значимости (из главы 2.4)	Перенормированный коэффициент значимости	Вычисленное значение
		0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	Н/О			
1	Проводится ли проверка персонала перед устройством на работу?											1		0,2	0,21	0,21
2	Предусмотрена ли административная ответственность персонала за нарушение конфиденциальности?											1		0,4	0,42	0,42
3	Предусмотрены ли меры и средства контроля за персоналом?											1		0,2	0,21	0,21
4	Проводится ли обучение персонала в области ИБ?						1							0,05	0,05	0,03
5	Ведется ли мониторинг за действиями сотрудников, работающих с ПД?												1	0,05	0,00	0,00
6	Прописаны ли обязанности руководства по надлежащему контролю в сфере ИБ?								1					0,05	0,05	0,04
7	Отражает ли регламент работы политику ИБ?	1												0,05	0,05	0,00
Итоговая оценка критерия:																0,91

Рисунок Б.5 - Таблица для ввода ответов на вопросы критерия М5 и вывод значения оценки соответствия критерия

М6 – Оценка риска															
№ вопр.	Вопрос к критерию	Ответ на вопрос в вероятностной форме												Коэф. Значимости (из главы 2.4)	Перенормированный коэффициент значимости	Вычисленное значение
		0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	Н/О			
1	Принят ли регламент оценки рисков?	1												0,3	0,33	0,00
2	Проводится ли ежегодный аудит ИБ?	1												0,2	0,22	0,00
3	Разработаны ли шкалы оценки риска?	1												0,1	0,11	0,00
4	Проводится ли работа по улучшению и уточнению оценки по уже выявленным инцидентам?									1				0,1	0,11	0,09
5	Учитывается при оценке рисков заключения экспертов сферы ИБ?											1		0,1	0,11	0,11
6	Учтена ли процедура оценки рисков в документах нормативной базы администрации?				1									0,1	0,11	0,03
7	Утверждена ли методика оценки рисков ИБ в ФСБ/ФСЭК?												1	0,1	0,00	0,00
Итоговая оценка критерия:																0,23

Рисунок Б.6 - Таблица для ввода ответов на вопросы критерия М6 и вывод значения оценки соответствия критерия

М7 - Обеспечение непрерывности рабочих процессов															
№ вопр.	Вопрос к критерию	Ответ на вопрос в вероятностной форме												Коэф. Значимости (из главы 2.4)	Перенормированный коэффициент значимости	Вычисленное значение
		0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	Н/О			
1	В ИС прописаны требования к непрерывности рабочих процессов (НРП)?											1		0,2	0,20	0,20
2	Применена ли система управления непрерывности рабочих процессов?											1		0,2	0,20	0,20
3	Проводится ли контроль непрерывности рабочих процессов?											1		0,1	0,10	0,10
4	Проводится ли анализ/аудит рисков и благоприятных возможностей?						1							0,2	0,20	0,10
5	Проводится ли планирование и контроль деятельности за работоспособностью оборудования сотрудниками?								1					0,1	0,10	0,07
6	Установлен ли регламент внедрение НРП?		1											0,1	0,10	0,01
7	Планировано ли постоянное улучшение НБ?										1			0,1	0,10	0,09
Итоговая оценка критерия:																0,77

Рисунок Б.7 - Таблица для ввода ответов на вопросы критерия М7 и вывод значения оценки соответствия критерия

М8 - Управление инцидентами															
№ вопр.	Вопрос к критерию	Ответ на вопрос в вероятностной форме												Коэф. Значимости (из главы 2.4)	Перенормированный коэффициент значимости	Вычисленное значение
		0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	Н/О			
1	Внедрена ли система управления инцидентами?											1		0,4	0,40	0,40
2	Утверждена ли программа менеджмента инцидентов НБ?											1		0,1	0,10	0,10
3	Обеспечивается ли техническая поддержка пользователей при возникновении инцидентов?								1					0,2	0,20	0,14
4	Внедрен ли регламент нормативных сроков устранение инцидентов?						1							0,05	0,05	0,03
5	Присутствует ли система обнаружения и оповещения о событиях ИБ?					1								0,1	0,10	0,04
6	Внедрена ли система ГосСОПКИ?										1			0,1	0,10	0,09
7	Предусмотрена ли сотрудник быстрого реагирования на инциденты?	1												0,05	0,05	0,00
Итоговая оценка критерия:																0,80

Рисунок Б.8 - Таблица для ввода ответов на вопросы критерия М8 и вывод значения оценки соответствия критерия

Итоговая оценка					
М1	Система менеджмента ИБ	0,58	0,66	Уровень эффективности системы менеджмента ИБ	
М5	Безопасность, связанная с сотрудниками	0,91			
М6	Оценка риска	0,23			
М7	Обеспечение непрерывности рабочих процессов	0,77			
М8	Управление инцидентами	0,80			
М2	Защита персональных данных граждан (контрагентов)	0,80	0,80	Уровень защиты ПД	
М4	Физическая безопасность	0,41	0,41	Уровень физической защиты	
М3	Управление доступом	0,51	0,51	Уровень ограничения доступа к ИСПД	
				Итоговая оценка	0,41

Рисунок Б.9 - Таблица объединения критериев в логические группы, с выводом значения оценки соответствия по этим группам и итоговой оценки

Приложение В – Результаты постпроектного анализа ИБ

Итоговая оценка					
M1	Система менеджмента ИБ	0,85		Уровень эффективности системы менеджмента ИБ	
M5	Безопасность, связанная с сотрудниками	0,91			
M6	Оценка риска	0,91	0,85		
M7	Обеспечение непрерывности рабочих процессов	0,77			
M8	Управление инцидентами	0,80			
M2	Защита персональных данных граждан (контрагентов)	0,98	0,98	Уровень защиты ПД	
M4	Физическая безопасность	0,93	0,93	Уровень физической защиты	
M3	Управление доступом	0,95	0,95	Уровень ограничения доступа к ИСПД	
				Итоговая оценка	**0,85**

Рисунок В.1 - Таблица вывода итоговой оценки постпроектного состояния

Приложение Г – Список сокращений и терминов

ВКР	-	Выпускная квалифицированная работа
ИТ	-	Информационные технологии
ИСПДн	-	Информационная система персональных данных
ПО		Программное обеспечение
МСУ	-	Муниципальное самоуправление
ПДн	-	Персональные данные
ИБ	-	Информационная безопасность
ЗЛВС	-	Защищенная локальная вычислительная сеть
СКУД	-	Система контроля и управления доступом
ИС	-	Информационная система
УБПДн	-	Угроза безопасности персональных данных
СУИБ	-	Система управления информационной безопастности
СМИБ	-	Система мониторинга информационной безопастности
НРП	-	Непрерывность рабочих процессов
IDS/IPS	-	Intrusion Detection System, системы обнаружения/предотвращения вторжений
APT	-	Advanced persistent threat, развитая устойчивая угроза
MSAT	-	Microsoft Security Assessment Tool