МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Программной инженерии

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Специализация Программирование интернет-приложений

**Отчет**

по лабораторной работе «Разработка политики информационной

безопасности гостиницы»

Выполнил студент Зинович Елизавета Игоревна

(Ф.И.О.)

Преподаватель ассистент Копыток Дарья Владимировна

(учен. степень, звание, должность, подпись, Ф.И.О.)

**Актуальность, цели и задачи разработки ПИБ**

Без решения задач информационной безопасности не может продолжать работу ни одно из предприятий, в том числе и гостиница. В любой организации возникает проблема безопасного хранения, передачи, использования информации.

Целью обеспечения информационной безопасности автоматизированной системы управления технологическими процессами является повышение уровня устойчивости ее функционирования, стабильности исполнения реализуемых технологических процессов путем предотвращения и/или снижения возможного ущерба от несанкционированных воздействий на объекты защиты автоматизированной системы управления технологическими процессам.

Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

**Структура организации**

Структура гостиницы представлена на рисунке 1.1.



Рисунок 1.1 - Структура компании

Текущее руководство осуществляет управляющий гостиничным комплексом.

Менеджеры всех отделов подотчетны директору. Каждый отдел также разбивается на более мелкие организационные единицы.

Менеджер административной службы должен, во-первых, обладать всей возможной информацией о гостинице. Во-вторых, он должен уметь четко планировать работу администрации. В-третьих, должен осуществлять постоянный контроль за работой своего отдела. Все вопросы, проблемы и недоразумения гостей должны разрешаться также с его помощью.

Служба питания. В гостинице имеется круглосуточный магазин, кофе-бар. Поступление продуктов питания на кухню осуществляется следующим образом. Продукты, чаще всего в виде полуфабрикатов, поступают на склад и/или в холодильник. Затем по мере надобности они поступают в отдел переработки, где осуществляется первичная готовка. Окончательное блюдо делают либо в горячем цехе, либо в кондитерском отделе.

Обслуживание в номерах непосредственно относится к подразделению питания. Официанты по заказу клиента доставляют к нему в номер блюда и напитки. Работа осуществляется следующим образом. Гость звонит в эту службу. Официантка принимает заказ и направляет его на кухню, где он выполняется. Затем она забирает заказ и доставляет его гостю в номер. Спустя некоторое время, официантка звонит гостю и спрашивает, можно ли забрать пустые тарелки и приборы. Также в ведении службы обслуживания в номерах находятся и мини-бары, которые есть в каждом номере.

**Основные угрозы и их источники**

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

Множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения:

* антропогенные,
* техногенные
* естественные (природные).

Антропогенные угрозы напрямую связаны с деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, — так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека. К естественным угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

Источники угроз по отношению к инфраструктуре гостиницы могут быть как внешними, так и внутренними.

Источниками внутренних угроз могут являться:

* сотрудники гостиницы;
* программное обеспечение;
* аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

* ошибки пользователей и системных администраторов;
* нарушения сотрудниками гостиницы установленных регламентов сбора, обработки, передачи и уничтожения информации;
* ошибки в работе программного обеспечения;
* отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

* компьютерные вирусы и вредоносные программы;
* организации и отдельные лица;
* стихийные бедствия.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:

* информационные;
* программные;
* физические.

К информационным угрозам относятся:

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* хищение информации из архива, отделов и баз данных;
* нарушение технологии обработки информации;
* противозаконный сбор и использование информации;
* использование информационного оружия.

К программным угрозам относятся:

* использование ошибок в ПО;
* компьютерные вирусы и вредоносные программы.

К физическим угрозам относятся:

* уничтожение или разрушение средств обработки информации и связи;
* хищение носителей информации;
* хищение программных или аппаратных ключей и средств криптографической защиты данных;
* воздействие на персонал (шантаж, нападение).

Специфические угрозы безопасности:

* возможность отключения электричества в гостинице, что приведет к сбою незавершенных операций и потерям в базах данных;
* угроза передачи носителей и паролей к ним сотрудниками гостиницы третьим лицам;
* угроза возникновения ошибок при передаче информации от других государственных учреждений;
* угроза передачи сотрудниками гостиницы информации о счетах плательщика, прибыли и выручке третьим лицам;
* угроза разглашения личной информации, контактных данных, идентификационных сведений граждан, сведений о регистрации движимого и недвижимого имущества;
* угроза проникновения на рабочие места сотрудников гостиницы людей, не являющихся работниками отделов, которые имеют туда доступ;
* угроза доступа в ИТ-отделе, изменения настроек сетевых параметров и потоков передачи данных между структурами;
* угроза взлома персональных страниц плательщиков в системе электронной подачи деклараций и т.д.

Реализация организационно-технических мер обеспечения информационной безопасности достигается в первую очередь путем:

* наделения пользователей автоматизированной системы управления технологическими процессами правами доступа и привилегиями по работе в;
* корректного использования и администрирования встроенных механизмов безопасности технических средств обработки, хранения и передачи информации и средств защиты;
* контроля функционирования и настроек механизмов безопасности, а также соблюдения требований по информационной безопасности;
* физической защиты технических средств обработки, хранения и передачи информации от неправомерного доступа к ним.
* Обязанности пользователей по обеспечению информационной безопасности зависят от занимаемой должности и определены в их должностных инструкциях.
* Угроза безопасности, потенциальное нарушение безопасности, любое обстоятельство или событие, которое может является причиной нанесения ущерба предприятию в целом.

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные). Естественные угрозы – это угрозы, вызванные воздействиями на предприятие объективных физических процессов или стихийных природных явлений, независящих от человека. Искусственные угрозы – это угрозы предприятию, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

* непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
* преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к предприятию могут быть внешними или внутренними (составляющие самой организации – её аппаратура, программы, персонал, конечные пользователи).

Основные непреднамеренные искусственные угрозы предприятию (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

* неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
* неправомерное отключение оборудования или изменение режимов работы устройств и программ;
* неумышленная порча носителей информации;
* запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
* нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
* заражение компьютера вирусами;
* неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
* разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
* проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
* игнорирование организационных ограничений (установленных правил) при работе в системе;
* вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
* некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
* пересылка данных по ошибочному адресу абонента (устройства);
* ввод ошибочных данных;
* неумышленное повреждение каналов связи.

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

* физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);
* отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
* действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
* внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
* вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
* применение подслушивающих устройств, дистанционная фото- и видео-съемка и т.п.;
* перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сели питания, отопления и т.п.);
* перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
* хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);
* несанкционированное копирование носителей информации;
* хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
* чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
* чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой зашиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;
* незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
* несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
* вскрытие шифров криптозащиты информации;
* внедрение аппаратных «спецвложений», программных «закладок» и «вирусов» («троянских коней» и «жучков»), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
* незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
* незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

**Оценка угроз, рисков и уязвимостей**

В рамках деятельности по обеспечению информационной безопасности условная численная шкала для оценки ущерба гостинице от НСД следующая:

Таблица 1.1 - Численная шкала для оценки ущерба гостинице от НСД

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб гостинице |
| 1 | Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение гостиницы на рынке не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время гостиницпа терпит убытки. |
| 3 | Значительные потери на рынке и в прибыли. От гостиницы уходит ощутимая часть клиентов |
| 4 | Потери очень значительны, гостиница на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы |
| 5 | Гостиница прекращает существование |

В рамках деятельности по обеспечению информационной безопасности вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам следующая.

Таблица 2 - Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НДС) |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

В рамках деятельности по обеспечению информационной безопасности оценка рисков следующая:

Таблица 3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб x Вероятность) |
| Спам | 1 | 0,4 | 0,4 |
| Копирование жесткого диска из центрального офиса | 3 | 0,1 | 0,3 |
| Межсайтовое кодирование (XSS-атаки) | 2 | 0,1 | 0,2 |
| SQL-инъекции | 2 | 0,1 | 0,2 |
| Вирусы | 2 | 0,3 | 0,6 |
| DDoS-атаки | 2 | 0,3 | 0,6 |
| Неправильная конфигурация web-сервера | 1 | 0,1 | 0,1 |
| Пиратское ПО | 3 | 0,1 | 0,3 |
| Итого | 16 | 1,5 | 2,7 |

**Меры, методы и средства обеспечения требуемого уровня**

**защищенности информационных ресурсов**

Комплексная система обеспечения безопасности информации в гостинице должна обеспечивать сохранность персональных данных, а также информации о структуре используемых технических и программных средствах, о структуре, принципах и алгоритмах работы средств защиты информации.

Комплексная система обеспечения безопасности персональных данных в гостинице включает в свой состав следующие группы мер и мероприятий по защите информации:

* правовые и законодательные; к ним относятся действующие законы и иные правовые нормативные акты, регламентирующие правила обращения с информацией, устанавливающие права и обязанности участников процессов обработки и использования информации и определяющие ответственность и санкции за нарушения этих правил. Важным условием использования данных мер защиты, является обеспечение осведомленности пользователей о действующих требованиях.
* организационные и административные; регламентируют процессы функционирования, использование ещё ресурсов, деятельность обслуживающего персонала гостиницы (формирование политики информационной безопасности и формулировку перспектив дальнейшего развития и совершенствования системы защиты информации; определение регламента и процедуры предоставления доступа к ресурсам; определение порядка взаимодействия и координация действий всех подразделений гостиницы с целью обеспечения требуемого уровня защищённости информационных ресурсов; определение обязанностей пользователей и степень ответственности за нарушения процедур обработки данных и защиты информации; осуществление контроля над выполнением положений нормативных документов и проведение проверок; подбор и проверку персонала при зачислении в штат организации и предоставлении доступа к информационным ресурсам; проведение мероприятий по доведению порядка эксплуатации компонент АС до пользователей (проведение инструктажа);
* режимно-объектовые; основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, предназначенных для предотвращения физического проникновения потенциальных нарушителей к компонентам системы и защищаемым информационным ресурсам, а также технических средств наблюдения, связи, охранной и пожарной сигнализации.

Для обеспечения физической безопасности компонентов выполняются следующие организационные и технические мероприятия: введение ограничений по доступу в помещения гостиницы, предназначенные для хранения и обработки персональных данных; оборудование системы устройствами от сбоев электропитания и помех в линиях связи; контроль доступа сотрудников и посторонних лиц в помещения гостиницы.

* технические и технологические; в системы технических и технологических средств защиты входят следующие подсистемы: подсистема защиты информации от НСД; подсистема антивирусной защиты; подсистема обнаружения вторжений; подсистема анализа защищенности; подсистема межсетевого экранирования.

Технические меры защиты информации конфиденциального характера, при ее передаче и обработке техническими средствами устанавливаются в соответствии с требованиями действующего законодательства и внутренними нормативными документами, регламентирующими организацию технической защиты информации конфиденциального характера в гостинице.

Для построения комплексной системы защиты информации необходимо разработать модель угроз и модель нарушителя, на ее основании разработать систему защиты информации, обеспечивающую противодействие актуальным угрозам безопасности, при этом необходимо учесть следующие требования:

* применяемые средства и технологии защиты должны обладать свойствами модульности, масштабируемости, открытости и возможности адаптации системы к различным организационным и техническим условиям;
* подсистемы и компоненты средства защиты информации должны обеспечивать безопасное функционирование всех элементов (серверного и системногопрограммного обеспечения, прикладных систем, систем связи);
* должен быть предусмотрен комплекс организационно-технических мер и мер технологической защиты информации.

Комплексная система защиты информации по своей структуре подразделяется на ряд составляющих ее подсистем, основывающихся на различных механизмах защиты и объединенных единой идеологией построения и управления. Только совокупность защитных механизмов всех подсистем позволяет осуществить комплексное обеспечение информационной безопасности.

При сборе, обработке, хранении, использовании и передаче персональных данных в гостинице обеспечивается следующее:

* доступ к персональным данным только для специально уполномоченных лиц, при этом указанные лица должны получать только те данные, которые необходимы для выполнения конкретных функций;
* проведение мероприятий, направленных на предотвращение НСД к персональным данным и (или) передачи ее лицам, не имеющим права доступа к такой информации;
* своевременное обнаружение фактов несанкционированного доступа к персональным данным;
* недопущение воздействия на технические средства автоматизированной обработки информации, в результате которого может быть нарушено их функционирование;
* постоянный контроль обеспечения защищенности информации.

На структурное подразделение или должностное лицо, ответственное за обеспечение информационной безопасности гостиницы возлагаются следующие задачи:

* методологический контроль в области безопасности информации;
* взаимодействие с государственными органами в части защиты информационных ресурсов от НСД,
* сертификации используемых технических средств и аттестации объектов информатизации по требованиям безопасности информации;
* взаимодействие с правоохранительными органами в части расследования компьютерных инцидентов и преступлений в области информационных технологий.

В структурных подразделениях разрабатывается перечень должностных обязанностей работников, ответственных за обеспечение безопасности конфиденциальной информации.

В целях предотвращения несанкционированного доступа к информации и ее утечки, хищения технических средств обработки и хранения информации и несанкционированного управления ими обеспечивается физическая защита входящих в нее технических средств.

Серверное оборудование и критичное сетевое оборудование гостиницы размещаются в запираемых шкафах с сигнализацией, располагаемых в специализированных помещениях (серверных), ограничивающих доступ к ним посторонних лиц.

Перед утилизацией или передачей в ремонт технических средств выполняется гарантированное удаление информации с них.

Кабельные сети в гостинице прокладываются так, чтобы максимально ограничить несанкционированный доступ к ним.

Для защиты от перебоев электричества в гостинице в эксплуатацию вводятся централизованные системы бесперебойного питания. Система информационной безопасности включает в себя максимальное количество элементов, обеспечивающих эффективную защиту системы при критической нагрузке.

В целях обеспечения безопасности технических средств автоматизированной системы управления технологическими процессами осуществляется защита зданий, сооружений и помещений гостиницы. Здания и сооружения, в которых размещаются технические средства гостиницы, обеспечиваются инженерно-техническими средствами охраны и средствами защиты от противоправных действий.

Помещения, в которых размещаются критически важные технические средства гостиницы, оборудуются средствами пожарной безопасности, вентиляции и кондиционирования. Доступ в такие помещения разрешается работникам гостиницы только для выполнения должностных обязанностей по обслуживанию технических средств. Доступ в помещения ограничивается средствами контроля и управления доступом. При выполнении работ в помещениях, где размещаются критически важные технические средства автоматизированной системы управления технологическими процессами, лицами, чья деятельность не связана непосредственно с их обслуживанием, обеспечивается контроль их деятельности.

Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации в гостинице разделяются и возлагаются на специально выделенных для этого работников. Изменения конфигурации средств обработки и хранения информации, а также изменения сетевой инфраструктуры, конфигурации сетевого оборудования выполняются администратором. Все изменения регистрируются в соответствующих журналах. Самостоятельное изменение конфигурации средств обработки, хранения.

Использование съемных носителей информации в автоматизированной системе управления технологическими процессами гостиницы запрещено. При размещении средств разработки, тестирования и эксплуатации обеспечивается их физическое или логическое разделение в целях снижения риска несанкционированного доступа или внесения изменений в систему.

В целях предотвращения проникновения, обнаружения внедрения и нейтрализации вредоносного ПО в оборудование гостиницы применяются средства защиты от вредоносного ПО. Средства защиты от вредоносного ПО устанавливаются на серверном оборудовании и оборудовании специалистов автоматизированной системы управления технологическими процессами. Управление и обновление средств защиты от вредоносного ПО осуществляются централизованно. Разрешается использование только сертифицированных на соответствие требованиям безопасности информации средств защиты от вредоносного ПО. Администрирование средств защиты от вредоносного ПО осуществляется системным администратором гостиницы. Настройки системы защиты от вредоносного ПО согласовываются и контролируются администратором ИБ.

Используемая антивирусная система защиты имеет:

* стойкую систему самозащиты, которая не позволит неизвестной вредоносной программе нарушить нормальную работу гостиницы;
* систему обновлений, находящуюся под контролем системы самозащиты антивирусной системы и не использующую компоненты операционной системы, которые могут быть скомпрометированы;
* систему обновления, позволяющую мгновенно, по сигналу системы централизованного управления доставить на защищаемый антивирусом объект обновления для лечения активного заражения;
* дополнительные механизмами для обнаружения новых неизвестных вредоносных программ;
* проверяет все поступающие из локальной сети файлы до момента получения их используемыми приложениями, что исключает использование вредоносными приложениями неизвестных уязвимостей данных приложений;
* систему централизованного сбора информации с удаленных рабочих станций и серверов, позволяющую максимально быстро передавать в антивирусную лабораторию всю необходимую для решения проблемы информацию.

В целях обеспечения непрерывного и устойчивого функционирования гостиницы осуществляется защита ее сетевой инфраструктуры.

Защита сетевой инфраструктуры обеспечивается:

* физической защитой сетевого оборудования и средств защиты гостиницы;
* контролем логического доступа к сетевому оборудованию гостиницы;
* шифрованием каналов управления;
* контролем сетевых соединений;
* обнаружением и предотвращением вторжений;
* мониторингом подключаемых к ЛВС автоматизированной системы управления технологическими процессами сетевых устройств;
* использованием встроенных в сетевое оборудование средств защиты от подмены адреса;
* защитой информации ограниченного доступа при ее передаче вне контролируемых зон;
* применением средств мониторинга и регистрации событий.

Контроль сетевых соединений между ЛВС гостиницы и подключаемыми к ней беспроводными сетями также осуществляется средствами межсетевого экранирования.

Защита информации ограниченного доступа при ее передаче вне контролируемых зон осуществляется применением сертифицированных средств криптографической защиты информации (построением защищенных виртуальных сетей). Защита от вторжений в ЛВС гостиницы осуществляется средствами обнаружения и предотвращения вторжений, размещаемыми на входе. Базы данных сигнатур средств обнаружения и предотвращения вторжений регулярно обновляются с сайта производителя применяемых средств. Категорически запрещается удаленное администрирование гостиницы.

В целях поддержания работоспособности ПО в гостинице осуществляются меры по устранению уязвимостей ПО, а также другие меры защиты от:

* умышленного либо неумышленного раскрытия, модификации или уничтожения защищаемых данных. В частности, это подразумевает использование средств ограничения доступа к различным ресурсам офисного контроля;
* установки средств защиты кем-либо, кроме системного администратора гостиницы, несанкционированного внесения изменений в порядок функционирования системы защиты, изменения ее возможностей. Данное требование приводит к необходимости разграничения прав доступа к настройкам системы, защите ее от несанкционированного воздействия. Это подразумевает использование в локальной сети только программных продуктов, поддерживающих ролевой принцип доступа, а также применение функций офисного контроля.

Средства защиты должны устанавливаться как на рабочие станции гостиницы, так и на сервер. В гостинице, соответствующей требованиям стандарта, должна использоваться только защищенная почта, что вместе с требованием о наличии защиты от вирусов и спама подразумевает установку средств антивирусной фильтрации почтовых сообщений. В свою очередь доступ в сеть Интернет должен использоваться только для обеспечения банковской деятельности. Устранение уязвимостей ПО достигается регулярным централизованным получением и установкой обновлений, предоставляемых разработчиками ПО. Обновление ОС, другого общесистемного и прикладного ПО осуществляется системными администраторами гостиницы и администраторами прикладных систем. Обновления для ПО получаются с серверов обновлений.

В целях обеспечения конфиденциальности информации при ее передаче вне контролируемых зон применяются сертифицированные установленным порядком средства криптографической защиты информации. Это специальные методы шифрования, кодирования в результате которых содержание передаваемых файлов становится недоступным, без предъявления ключа криптограммы и обратного преобразования.

Криптографическая защита информации в гостинице реализована с помощью метода криптосистемы с открытым ключом. В системе с открытым ключом используются два ключа — открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

В целях обеспечения безопасности информационных ресурсов и устойчивого функционирования автоматизированной системы управления технологическими процессами осуществляется управление доступом пользователей к операционным и прикладным системам, а также сетевому оборудованию гостиницы. Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач. Наделение пользователей правами доступа и привилегиями основывается на установленной в формализованной процедуре предоставления прав доступа. Права доступа и привилегии пользователей подлежат регулярному пересмотру. Каждый пользователь обеспечивается уникальным персональным идентификатором. Подтверждение подлинности идентификатора (аутентификация) пользователя осуществляется при помощи паролей и/или средств усиленной аутентификации. Длина, сложность и срок действия паролей устанавливаются в зависимости от степени критичности защищаемых систем.

**Выводы**

Политика безопасности гостиницы описывает порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Разработаны технические меры обеспечения безопасности, организационные меры обеспечения безопасности, сетевая безопасность, общие меры предосторожностей для гостиницы.

Политика информационной безопасности необходима для обоснования введения защитных мер в компании. Политика должна быть утверждена высшим административным органом компании (генеральный директор, совет директоров и т.п.).