Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

политики информационной

безопасности интернет–магазина «ICiens»

**Выполнил:**

студент 3 курса 8 группы

специальности ПОИБМС

Ярмолик Н.С.

**Проверил:**

Берников В.О.

Минск 2020

1. **Обоснование актуальности, цели и задачи ПИБ в интернет–магазине**

Деятельность любой организации в наше время связана с получением и передачей информации. Информация в настоящее время является стратегически важным товаром. Потеря информационных ресурсов или завладение секретной информацией конкурентами, как правило, наносит предприятию значительный ущерб и даже может привести к банкротству. За последние 20 лет информационные технологии проникли во все сферы управления и ведения бизнеса. Сам же бизнес из реального мира давно переходит в мир виртуальный, а поэтому весьма зависим от вирусных, хакерских и прочих атак.

В наше время торговля посредством сети интернет развивается достаточно быстро. Данный способ торговли становится все более актуальным, особенно там, где электронным рынком можно воспользоваться большей части предприятий.

Создание Интернет-магазинов стало общедоступно для всех пользователей сети Интернет, за данный вид коммерции взялись и различные фирмы, более того появились компании, полностью интегрировавшие свою коммерческую деятельность во Всемирную паутину. Из выше сказанного можно сделать вывод, что всё более распространено понятия того, что интернет-магазин – лицо компании.

На текущий момент актуально понятие того, что интернет-магазин представляет собой одну из составляющих коммерческой фирмы. Каждый день регистрируются десятки взломов. Многие компании с особым вниманием рассматривают вопросы безопасности, так как современные прогрессивные темпы развития и деятельность в конкурентной среде не оставляют другого выбора.

Под информационной безопасностью понимается состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.

При обеспечении информационной безопасности должен соблюдаться ряд основных требований – доступность, конфиденциальность, целостность. Любая угроза информационной безопасности должна рассматриваться с точки зрения того, как она может повлиять на данные требования. Однако рост количества и качества угроз безопасности информации в компьютерных системах не всегда ведет к адекватному ответу на создание надежной системы и безопасных информационных технологий.

Одной из актуальных проблем информационной безопасности на современном этапе является проблема определения и реализации требуемого уровня защищённости компьютерных систем, обрабатывающих конфиденциальную информацию.

Из всего выше сказанного можно сделать вывод, что информационная безопасность интернет-магазина является одним из важных и актуальных аспектов его существования в целом.

Настоящая Политика является основополагающим документом, регулирующим деятельность интернет–магазина «ICiens» в области информационной безопасности.

Данный документ разработан для обоснования актуальности разработки ПИБ в интернет–магазине и определяет цели и задачи её разработки.

Цель разработки информационной безопасности – создание и постоянное соблюдение в интернет–магазине «ICiens» условий, при которых риски, связанные с нарушением безопасности информационных активов интернет-магазина, постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне остаточного риска.

Процессы обеспечения информационной безопасности интернет–магазина «ICiens» являются составной и неотъемлемой частью процессов управления информационными технологиями и сопутствующими операционными рисками.

В области разработки политики информационной безопасности интернет–магазином «ICiens» является разработка следующих стратегических целей:

* Повышение конкурентоспособности бизнеса «ICiens».
* Соответствие требованиям законодательства и договорным обязательствам в части информационной безопасности.
* Повышение деловой репутации и корпоративной культуры «ICiens».
* Эффективное управление информационной безопасностью и непрерывное совершенствование системы управления информационной безопасностью.
* Достижение адекватности мер по защите от угроз информационной безопасности.
* Обеспечение безопасности корпоративных активов «ICiens», включая персонал, материально-технические ценности, информационные ресурсы, бизнес-процессы.

Указанная цели достигаются посредством обеспечения (поддержания) следующих свойств информации при её автоматизированной обработки:

* доступности обрабатываемой информации для зарегистрированных пользователей, устойчивого функционирования системы, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время.
* сохранения в тайне (обеспечения конфиденциальности) определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи.
* целостности и аутентичности информации, хранимой, обрабатываемой и передаваемой по каналам связи.

В области разработки политики информационной безопасности интернет–магазином «ICiens» является реализация следующих задач:

* Вовлечение высшего руководства «ICiens» в процесс обеспечения информационной безопасности: деятельность по обеспечению информационной безопасности инициирована и контролируется высшим руководством «ICiens».
* Соответствие требованиям законодательства РБ: «ICiens» реализует меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством и договорными обязательствами.
* Применение экономически целесообразных мер: «ICiens» стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации.
* Проверка работников: все кандидаты на вакантные должности в «ICiens» в обязательном порядке проходят проверку в соответствии с установленными процедурами.
* Документированность требований информационной безопасности: в «ICiens» все требования в области информационной безопасности фиксируются в разрабатываемых внутренних нормативных документах.
* Повышение осведомленности в вопросах обеспечения информационной безопасности: документированные требования в области информационной безопасности доводятся до сведения работников всех бизнес-подразделений «ICiens» и контрагентов в части их касающейся.
* Реагирование на инциденты информационной безопасности: «ICiens» стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения информационной безопасности.
* Оценка рисков: в «ICiens» на постоянной основе реализуются мероприятия по оценке и управлению рисками информационной безопасности, повышению уровня защищенности информационных активов.
* Учет требований информационной безопасности в проектной деятельности: помимо операционной деятельности, «ICiens» стремится учитывать требования информационной безопасности в проектной деятельности. Разработка и документирование требований по обеспечению информационной безопасности осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации.
* Постоянное совершенствование системы управления информационной безопасностью: совершенствование системы управления информационной безопасности является непрерывным процессом.

1. **Объекты защиты**

Современный интернет–магазин – это совокупность специализированных отделов, и в то же самое время – это деятельность по реализации процессов. Поэтому для описания любого бизнеса можно использовать два способа: функциональный и процессный. Процессный подход предполагает, что организация – это совокупность взаимосвязанных и взаимодействующих процессов.

Составляющими организационных структур являются:

* элементы организационных структур управления – службы или органы аппарата управления, а также отдельные работники этих служб (органов);
* организационные отношения – отношения (связи) между подразделениями организации, уровнями ее управления, персоналом, посредством которых реализуются функции управления;
* уровни управления – совокупность прав, обязанностей и ответственности, характерная для должностных лиц, занимающих определенную ступень в иерархической структуре организации.

Структура управления интернет–магазина построена именно таким образом с целью обеспечения максимальной сегментации отделов и недопущения утечки данных сотрудникам, не имеющим прямого к ним отношения. Данная схема способствует обеспечению корректной работы внутри компании, защиты ее интересов, при этом соблюдая интересы клиентов, обеспечивая право на защищенность личных данных.

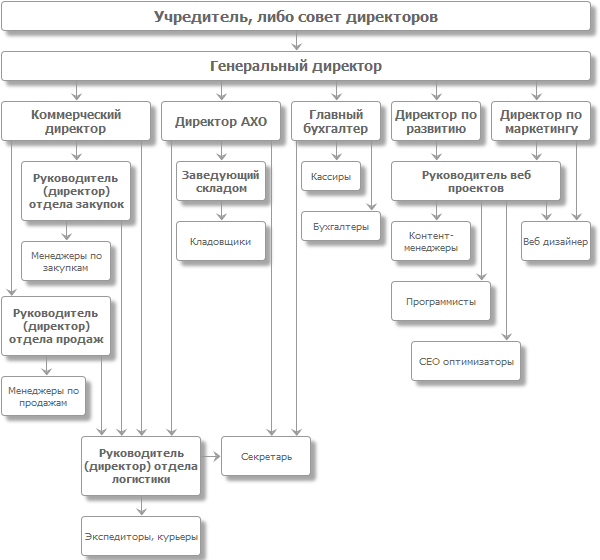


Рисунок 2.1 – Организационная структура интернет–магазина

Проработка структуры демонстрирует четкую сегментацию на отделы, которые взаимодействуют между собой только через исполнительного директора и владельца бизнеса.

**Совета директоров** не занимается оперативной работой, но созывает и ведет совет директоров.

**Генеральный директор** — это управляющий всей деловой жизнью интернет–магазина. Он принимает оперативные решения, руководит всей службой отделов, налаживает связи с властями и другими сторонними организациями.

**Директора –** управляют отдельными частями компании и отвечают за определенные отделы

**Главный бухгалтер –** Специалист по организации бухгалтерского учета хозяйственно-финансовой деятельности и контролю за экономным использованием материальных, трудовых и финансовых ресурсов, сохранностью собственности предприятия.

**Руководители определенных отделов –** непосредственно взаимодействуют с персоналом организовывая их работу в соответствии с планом высшего руководства. Это наиболее квалифицированные специалисты, которым поручается руководство узкоспециализированной группой или участком и которые оказывают помощь рядовым работникам, разрешают спорные и сложные вопросы, дают консультации по конкретным случаям, занимаются обучением персонала

**Персонал третьего уровня** — непосредственные работники. Выполняют указания руководителей отделов и отвечают за непосредственное выполнение поставленных компанией целей.

В интернет–магазине циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (служебная, коммерческая, персональные данные), и открытые сведения.

Защите подлежит вся информация и информационные ресурсы интернет–магазина, независимо от ее представления и местонахождения в информационной среде магазина:

* сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации в соответствии с законом.
* сведения о частной жизни граждан (персональные данные), доступ к которым ограничен в соответствии с законом.
* открытая информация, необходимая для обеспечения нормального функционирования интернет–магазина.

**Объектами** защиты будут выступать пассивные компоненты системы, хранящий, перерабатывающий, передающий или принимающий информацию. Примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, жесткие диски (или твердотельные накопители), серверное оборудование, принтеры, коммутационное оборудование и т.д.).

В первую очередь объектом защиты будет являться система онлайн-заказа товара и банковские данные передаваемые посредствам веб-сайта. При атаке на данный объект компания понесет огромные материальные и репутационные потери. Поэтому необходима надежная защита от фишинговых атак и несанкционированного доступа с правами администратора или посредствам уязвимостей в устаревшем программном обеспечении, а также аудит системы на предмет утечки информации.

Вторым объектом защиты по значимости будет личная информация пользователя, т.к. при несанкционированном доступе к ней компания, в первую очередь, потеряет свой статус для пользователя. Личной информацией может являться следующее: пароль, телефон, адреса, банковские данные, паспортные данные. Потеря такой информации может повлечь крайне серьёзные репутационные и материальные потери. Методами защиты является тоже самое разграничение доступа и аудит, для предотвращения или быстрого поиска виновника утечек, так же обслуживание оборудования (обновление прошивок и правильная настройка), обновление программного обеспечения на серверном оборудовании и компьютерной технике персонала, периодическая проверка о появлении новых уязвимостей и методов их закрытия.

Следующими объектами являются: файлы, папки, директории, компьютерные программы, сервера, устройства (мониторы, жесткие диски (или твердотельные накопители), серверное оборудование, принтеры, коммутационное оборудование и т.д.). Их защита должна быть как физической от не допуска или контроля доступа работника к оборудованию и носителям информации (смарт-замки, камеры), так и программной (шифрование, обязательная аутентификация пользователя, защита от копирования)

**Субъектами** информационных отношений являются пользователи, различные процессы или устройства, которые могут инициировать поток информации. В нашем случае это работники компании разных уровней, клиенты, программное обеспечение, получающее в автоматическом режиме данные от оборудования компании (системы статистики, парсеры, поисковые системы, банковские системы)

Веб-сайт должен быть защищён от атак разного рода, ведь приостановка его работы либо хищение данных может привести к потери данных, хищению или их изменению, а также к потери репутации и денег самой компании.

1. **Основные угрозы и их источники**

Угроза – это любое событие, которое потенциально может нанести вред организации путем раскрытия, модификации или разрушения информации, или отказа в обслуживании критическими сервисами. Угрозы могут быть неумышленными, такими как те, что вызываются ошибками человека, сбоями оборудования или программ, или стихийными бедствиями. Умышленные угрозы могут быть разделены на ряд групп: от логичных (получение чего-либо без денег) до иррациональных (разрушение информации).

**Естественные угрозы** – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;

**Искусственные угрозы** – это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

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

Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

Согласно данным компании «Positive Technologies», чаще всего выделяют следующие виды угроз:

* Межсайтовое кодирование (XSS –атаки);
* SQL – инъекции;
* Неправильная конфигурация web-сервера;
* Вредоносное программное обеспечение;
* Подделка межсайтовых запросов (CSRF);
* Вызов исключительных ситуаций;
* Атаки типа «отказ в обслуживании» (DoS-атаки).

Результатом успешной реализации угроз безопасности Интернет-магазину может быть утечка или уничтожение конфиденциальной данных (коммерческой информации, сведения о покупателях), заражение системы и в последующем компьютеров пользователей вредоносным программным обеспечение, недоступность клиентов к web-приложению.

Ко всему этому, компания теряет доверие клиентов, теряет деньги от потенциальных и/или несовершенных сделок, нарушается деятельность электронного магазина, затрачивает время, деньги и человеческие ресурсы на восстановление функционирования и всё это приводит к ослаблению репутации на рынке.

Угрозы, связанные с перехватом передаваемой информации (получение несанкционированного доступа к ней) посредством сети Интернет, присущи не только к Интернет-магазину. Особое значение представляет то, что в системах электронной коммерции хранятся сведения, несущие экономическое характер: номера кредитных карт, номера счетов, содержание договоров и подобные.

Исходя из сказанного, возникает необходимость в использовании средств и методов защиты информационных ресурсов интернет-магазина от НСД (несанкционированного доступа).

Таким образом, можно сделать вывод, что обеспечение информационной безопасности Интернет-магазина – это не только одно из важных требований успешного ведения электронного бизнеса, но и фундамент доверительных отношений между клиентом и кампанией. Торговля посредством сети Интернет предполагает активный обмен информацией, проведение открытых транзакций через незащищенную сеть общего доступа, которые невозможны без доверия между субъектами бизнеса.

Исходя из этого, обеспечение информационной безопасности подразумевает комплексный подход, включающий в себя такие задачи, как доступ к серверам и web-приложениям, аутентификация и авторизация пользователей, обеспечение конфиденциальности и целостности персональных данных, реализация электронной цифровой подписи и применение прочих мер обеспечения информационной безопасности.

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 и «дыр» 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)

1. **Оценка угроз, рисков, уязвимостей**

Оценка информационных рисков интернет–магазина выполняется по следующим основным этапам:

* идентификация и количественная оценка информационных ресурсов, значимых для работы юридической компании;
* оценивание возможных угроз;
* оценивание существующих уязвимостей;
* оценивание эффективности средств обеспечения информационной безопасности.

При этом информационные риски зависят от:

* показателей ценности информационных ресурсов;
* вероятности реализации угроз для ресурсов;
* эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности организации.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например, учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка политики безопасности требует учета специфики конкретных организаций.

Таблица 4.1 – Условная численная шкала для оценки ущерба школы от НСД

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 1 | Раскрытие данных принесет ничтожно малый моральный и экономический ущерб работе кампании |
| 2 | Ущерб от атаки есть, но основные операции и положения затронут не будут |
| 3 | Значительные финансовые потери и потери доверия со стороны клиента, ощутимая часть которых уйдет |
| 4 | Потери очень значительные, кампания теряет свое положение на рынке в долгосрочном периоде. Для восстановления бизнеса потребуются крупные финансовые займы |
| 5 | Кампания прекращает существование |

Таблица 4.2 – Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 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 |

С помощью данных таблиц можно рассчитать риски, которым могут быть подвержены компоненты системы. На этапе анализа таблицы риски задаются максимально допустимым уровнем (порогом) значением 1,0.

Таблица 4.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб \* Вероятность) |
| Спам (переполнение почтового ящика) | 1 | 0,2 | 0,2 |
| Действия внутреннего или внешнего злоумышленника | 4 | 0,4 | 1,6 |
| Хищение личных данных отдельного клиента сотрудником кампании | 3 | 0,1 | 0,3 |
| Утеря носителей информации | 2 | 0,3 | 0,6 |
| Несанкционированное распространение информации через поля и электрические сигналы, случайно возникшие в аппаратуре | 3 | 0,1 | 0,3 |
| Отказы системы электроснабжения | 3 | 0,3 | 0,9 |
| Воздействие мощных электромагнитных и электрических помех (промышленных и природных) | 3 | 0 | 0 |
| Удаление базы данных клиентов с главного компьютера | 1 | 0,1 | 0,1 |

Продолжение таблицы 4.3

|  |  |  |  |
| --- | --- | --- | --- |
| Хищение документов, определяющих ценообразование, отражающих стратегическое планирование в рамках интернет–магазина «Iciens» | 2 | 0,1 | 0,2 |
| Распространение исследований кампании | 2 | 0,1 | 0,2 |
| Взлом аккаунтов кампании в социальных сетях | 2 | 0,2 | 0,4 |
| Перебои в электроснабжении | 3 | 0,2 | 0,6 |
| Ненадежность программ, используемых кампанией для ведения внутренних процессов | 2 | 0,1 | 0,2 |
| Аппаратные ошибки в настройке локальной сети кампании | 3 | 0,1 | 0,3 |
| Хищение клиентской базы человеком внешним для кампании | 2 | 0,1 | 0,2 |
| Программные ошибки в настройке локальной сети кампании. | 2 | 0,1 | 0,2 |
| Недостаточная квалификация сотрудников | 3 | 0,1 | 0,3 |
| Итого | 2,4 | 0,16 | 0,4 |

Следуя данным, полученным в таблице, можно сделать вывод, что самые вероятные риски для данного учреждения – это действия внутреннего или внешнего злоумышленника и перебои в электроснабжении.

Исходя из сказанного, возникает необходимость в использовании средств и методов защиты информационных ресурсов интернет-магазина от НСД (несанкционированного доступа).

1. **Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов**

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Отдельный раздел законопроекта "О коммерческой тайне", посвященный организации защиты коммерческой информации, определяет необходимый комплекс мероприятий по ее защите:

* установление особого режима конфиденциальности;
* ограничение доступа к конфиденциальной информации;
* использование организационных мер и технических средств защиты информации;
* осуществление контроля за соблюдением установленного режима конфиденциальности.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации. Как правило, особый режим конфиденциальности подразумевает:

* организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
* установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;
* установление пропускного режима в помещения, содержащие носители конфиденциальной информации;
* закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
* установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);
* организацию ремонта технических средств обработки конфиденциальной информации;
* организацию контроля за установленным порядком.

Эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

* средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;
* средства, обеспечивающие защиту информации при передаче ее по каналам связи;
* средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
* средства, обеспечивающие защиту от воздействия программ-вирусов;
* материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако это способ требует значительных капитальных затрат и практически не применяется.

Обеспечение требуемой защиты информационных ресурсов предприятий в этих условиях достигается применением дополнительных инструментальных средств. К их числу относятся:

* средства анализа защищенности операционных систем и сетевых сервисов;
* средства обнаружения опасных информационных воздействий (атак) в сетях.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок, и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

Важно помнить, что прежде, чем внедрять какие-либо решения по защите информации, необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности. При этом политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки на интернет–магазин, можем выделить следующие рекомендации, следуя которым возможно снизить риски опасного воздействия и их последствий:

* четкая и строгая иерархия должностей и полномочий в кампании. Каждый должен заниматься строго своим заданием и не иметь доступа к данным, использование которых для него не является необходимым;
* строгий подбор сотрудников с привлечением при поиске специалиста на ответственную должность HR служб;
* защита корпоративной почты и базы данных с исследованиями и клиентскими данными;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников;
* использование лицензионных программных продуктов с постоянными обновлениями;
* разграничение доступа к финансовым отделам. Уборщица не должна знать номер банковского счета фирмы и тем более, его пароля;
* проведение регулярных бесед и инструктажей с сотрудника

При разработке Интернет-магазина, как и при разработке любого веб-проекта, необходимо понимать, что информационная безопасность является одним из важных требований для полноценного и стабильного функционирования Интернет-магазина, как системы.

При правильной настройке системы управления контентом, системы разграничении доступа, http-сервера и системном подходе при решении проблем информационной безопасности CMS, система работает стабильно и даёт возможность управления процессами обеспечения информационной системы.

Таким образом, можно сделать вывод, что внедрение данной системы в Интернет-магазин автоматизирует некоторые процессы информационной безопасности и сократить определённые риски, однако информационная безопасность требует комплексного подхода и чаще всего человеческий фактор играет большую роль в правильном обеспечении безопасности.

**Выводы**

Политика информационной безопасности – важный инструмент, которым нужно правильно пользоваться. Малейшая ошибка в организации ПИБ –может привести к серьёзным последствиям. Данная тема требует практики, приобретение навыков работы с ней. Мои предложения состоят в том, чтобы тщательно планировать ПИБ, т.к. часто компании и фирмы этим пренебрегают, теряя свой статус на рынке и деньги. Политика безопасности компании зависит от требований бизнеса и необходимого уровня сохранности информации.

Приведенные меры по защите информации являются примерными. В реальности, следует провести комплексную оценку с привлечением специализированных людей, которые являются экспертами в вопросах обеспечения информационной безопасности для проведения специальных тестов и экспериментов.

Политики информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию юридической компании в области ИБ.

Политики информационной безопасности регламентируют эффективную работу средств защиты информации. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политики информационной безопасности реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Разработка политики информационной безопасности необходима для того, чтобы определить стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить. Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности. При этом политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия.

В теоретической части работы приведены следующие рекомендательные меры, соблюдение которых поможет снизить ущерб при возникновении атаки:

* четкая и строгая иерархия должностей и полномочий в кампании. Наличие четких прописанных регламентов обязанностей для каждой должности;
* подписание договоров о неразглашении информации с сотрудниками, имеющими доступ к клиентским базам данных и данным исследований кампании;
* строгий подбор сотрудников с привлечением, при необходимости, HR агенств;
* защита главных баз данных кампании и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников, использование лицензионных продуктов;
* разграничение доступа к финансовым отделам;
* проведение регулярных бесед и инструктажей с сотрудниками;

Решение проблем обеспечения безопасности электронной коммерции в первую очередь связано с решением вопросов безопасности технологий, применяемых в ней, то есть с обеспечением информационной безопасности.

При обеспечении информационной безопасности должен соблюдаться ряд основных требований – доступность, конфиденциальность, целостность. Любая угроза информационной безопасности должна рассматриваться с точки зрения того, как она может повлиять на данные требования.