Практически любое предприятие на сегодняшний день требует введения определенных стандартов информационной безопасности для того, чтобы защитить свои данные и обеспечить стабильное функционирование предприятия.

Цели использования стандартов информационной безопасности:

1. обеспечение необходимого уровня качества продуктов, товаров и услуг;
2. обеспечения единых характеристик продуктов, товаров и услуг.

Зачастую необходимость соблюдения некоторых стандартов информационной безопасности закреплена законодательно. Реальные причины гораздо глубже — обычно стандарт является обобщением опыта лучших специалистов в той или иной области, и потому представляет собой надежный источник оптимальных и проверенных решений.

Основным критерием организации системы информационной безопасности на предприятии является стандартизация, без которой практически невозможно отлаженное и стабильное функционирование предприятия.

Стандартизация в области ИБ необходима по трем основным причинам:

1) необходимость выработки единых требований по ИБ (единый набор требований);

2) необходимость выработки единых подходов к решению проблем ИБ;

3) необходимость выработки единых качественных показателей для оценки безопасности ИС и средств защиты.

Потребители (заказчики) продуктов информационных технологий без стандартов не смогут сформулировать свои требования по ИБ производителям информационных систем (нужны какие-то критерии, показатели, единицы измерения ИБ и т.д.).

Производители продукции ИТ и средств защиты (программных, технических) нуждаются в стандартах для того, чтобы можно было бы объективно оценить свою продукцию с точки зрения обеспечения ИБ, то есть СЕРТИФИЦИРОВАТЬ ее. Им также необходим стандартный набор требований для того, чтобы ограничить

фантазию заказчика и заставить выбирать конкретные требования из этого набора.

В настоящее время существует довольно много стандартов, а также других нормативных и руководящих документов в области информационной безопасности.

Проблемой информационной компьютерной безопасности начали заниматься с того момента, когда компьютер стал обрабатывать данные, ценность которых высока для пользователя. С развитием компьютерных сетей и ростом спроса на электронные услуги ситуация в сфере информационной безопасности серьезно обострилась.
Существуют множественные примеры ситуаций, в которых несоответствие стандартам информационной безопасности влекло за собой в дальнейшем большие проблемы для компании или даже ее крах.

Несмотря на то, что с одной стороны информационно-коммуникационных технологий и автоматизация открывают огромные возможности, в том числе в развитии бизнеса или организации других аспектов социальной жизни, чем больше задействованы в этой деятельности информационные технологии, тем большему риску подвержена в дальнейшем компания.

К примеру, для организации, инфраструктура которой является территориально-распределенной, необходимы единые правила по обеспечению защиты, к примеру, может быть организована разработка профиля, описывающего правила доступа и обмена информацией с удаленными объектами.

Цель данного эссе -- выявить особенности организации систем информационной безопасности на предприятии, а также риски, связанные с неверной ее организацией.

Задачи эссе:

- Проанализировать последствия, которые могут быть вызваны плохой организацией информационной безопасности на предприятии.
- Выявить оптимальную модель организации информационной безопасности на предприятии.
- Сделать выводы относительно организации информационной безопасности на предприятиях, выявить рекомендации касаемо дальнейшего использования материалов этой работы.

Актуальность данной темы обусловлена глобализацией информационных процессов, и, как следствие, необходимостью выстроить систему защиты данных компаний, которые на сегодняшний день могут составлять большую часть активов самой компании.

Стоит обратиться к конкретным случаям, чтобы понять, как может влиять нарушения в области информационной безопасности на развитие тех или иных систем и предприятий -- социальных, экономических и технических.

Примеры инцидентов, вызванных нарушениями в области информационной безопасности.

За последнее время множество неприятных инцидентов было вызвано нарушениями в системе безопасности Elasticsearch.
От наиболее крупных утечек данных пострадали такие компании, как:

- специализирующаяся на информационной безопасности и управлении облачными данными американская компания Rubrik;
- американская аналитической компании Dow Jones;
- интернет-магазин Gearbest.

Помимо этого, произошли утечки крупной базы данных китайских соискателей вакансий, а также базы данных китайского сервиса Alibaba.

Защита персональных данных очень важна, а утечка таких данных как номера банковских счетов, ИНН, прочих личных данных, в особенности в случае с большими корпорациями, может быть фатальной для компании и нанести непоправимый урон бизнесу как экономически, так и репутационно, поскольку после громкого инцидента многие клиенты не захотят больше иметь дел с поставщиком услуг, который может допустить их утечку данных.
Регулярно случаются инциденты утечки данных крупных компаний, взлома хакерами баз данных подобных компаний, в результате чего акции этих корпораций обесцениваются и лояльность аудитории снижается. Это наносит большой урон бизнесу, поэтому соблюдение стандартов информационной безопасности эссенциально для корпораций, собирающих большое количество персональных данных пользователей.

Более половины случаев утечки данных происходит по инсайдерским причинам, то есть по вине сотрудников самих компаний.

В свою очередь соблюдение стандартов информационной безопасности обеспечивает компанию множеством преимуществ по сравнению с теми компаниями, которые не слишком беспокоятся о защите своих данных и поддержании качества.

На нынешнем этапе развития информационных технологий становится понятно, что для создания эффективно и слаженно работающих продуктов, например, банковских, необходимо обеспечение их безопасностью высокого уровня методов внедрения систем защит. При этом рекомендуются меры, соответствующие национальным стандартам, поскольку только путем введения единых для всех мер возможно обеспечить должную безопасность, особенно в таких важных отраслях, как экономика и банкинг.

С началом использования сверхмобильных коммуникационных устройств, позволяющих решать широкий спектр задач угрозы информационной безопасности стали гораздо серьезнее. Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.

Успешный вектор организации информационной безопасности на примере предприятия “ООО Дайджекс Технолоджи”

Предприятие было основано в 2000 году. Организации разных городов России и стран СНГ пользуются услугами этой компании, в том числе и клиенты из таких городов, как Казань, Санкт-Петербург, Москва, Нижний Новгород, Ижевск и прочие. Настолько масштабная деятельность запрашивает особенное отношение к информационной безопасности в компании, поскольку в базах данных компании сосредоточено большое количество самых различных персональных данных пользователей и не только.

Для соответствия требованиям информационной безопасности, требуется соблюдение следующих критериев:

1. Требуется задокументированная политика компании относительно сохранности персональных данных.

2. Принцип контроля должен строго соблюдаться.

Высшие звания руководства должны быть обязаны подписать документы о неразглашении коммерческих секретов компании.

Важно подчеркнуть, что чем больше людей имеют доступ к коммерческим секретам, вероятность возможности раскрытия, а также потери носителей этих данных возрастает.

Особое внимание следует уделить безопасности компьютерной информации.

Сегодня эта компания создала несколько баз данных: компании-клиенты (телефоны и домашние, и деловые); доставленный товар; база данных сотрудников организации, соглашения и др.

В любом случае, попадание в руки конкурентов такой информации крайне нежелательно. Чтобы предотвратить такое развитие событий, рекомендуется создавать пароли для доступа к каждой базе данных. При загрузке компьютера также рекомендуется поставить двухуровневую защиту.

В случае возникновения каких-либо проблем необходимо полностью контролировать процесс ремонта оборудования. Когда у программиста есть все, что необходимо для получения доступа к свободному диску, при попадании этой информации в руки недоброжелателя она может быть использована для различных целей, в том числе для вывода из строя оборудования компании.

Необходимо постоянно обновлять антивирусные программы, чтобы обнаруживать и обезвреживать вирусы на вашем компьютере.

Рекомендуется приобрести спецтехнику для уничтожения бумажной информации.

Особое внимание следует уделить вопросам найма новых сотрудников.

Также для создания оптимальной политики в области информационной безопасности необходимо регулярно проводить оценку рисков, что позволит как избежать расходов на введение лишних мер, так и оценить эффективность контрмер.

Сегодня во многих организациях существует особый подход к этому процессу, который связан со стремлением сохранить информацию о фирмах и не допустить ее выхода за пределы «человеческого фактора».

Заключение

В ходе данного эссе были проведены:

- исследование на тему необходимости введения стандартов информационной безопасности на предприятии
- анализ процесса организации системы информационной безопасности компании.

Из результатов, полученных в ходе исследования, можно сделать выводы о том, что действительно наличие хорошо отлаженной системы безопасности на предприятии очень значимо для полноценного функционирования предприятия. Особенно важно иметь надежную систему информационной безопасности тем компаниям, которые работают с личными данными клиентами, а также с финансами. В такой ситуации утечка данных либо вторжение хакеров в систему безопасности компании может оказаться фатальным для ее репутации, а также послужить причиной финансового ущерба -- причем потери могут быть не только со стороны компании, но и со стороны ее клиентов.

Данное эссе рекомендовано к прочтению людям, начинающим изучение информационной безопасности, желающим четко обозначить практическую пользу применения стандартов информационной безопасности. Кроме того, эссе содержит пример организации системы информационной безопасности на предприятии, поэтому может быть так или иначе полезно людям, заинтересованным в построении системы информационной безопасности для своей компании.