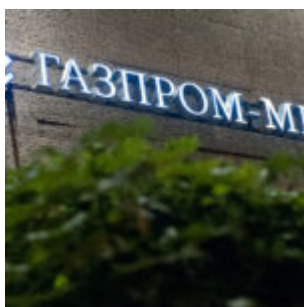


Повышение защищенности Microsoft Dynamics NAV в крупном медиа холдинге

написано GlobalTrust.ru | 24.07.2017



В четвертом квартале 2015 года компанией GlobalTrust был реализован проект по анализу защищенности, проектированию и внедрению системы защиты информационной системы Microsoft Dynamics NAV в одном из крупнейших российских медиа холдингов.

ERP-система Microsoft Dynamics NAV – это программное решение для управления финансовыми, кадровыми и прочими активами предприятия, позволяющее повысить эффективность бизнес-процессов. Данное решение используется для формирования и ведения штатного расписания; кадрового и персонифицированного учета; расчета заработной платы и налогов, а также взаимодействия с налоговыми органами и пенсионным фондом РФ.

В ходе выполнения работ специалистами GlobalTrust были решены следующие задачи:

- Разработка модели угроз и нарушителей информационной безопасности Microsoft Dynamics NAV;
- Анализ защищенности Microsoft Dynamics NAV и среды функционирования;
- Оценка надежности и полноты существующих контрмер, соответствие внутренним и международным стандартам;
- Подготовка рекомендаций по повышению защищенности Microsoft Dynamics NAV и среды функционирования;
- Проектирование и внедрение подсистемы защиты Microsoft Dynamics

NAV.

С целью решения данных задач специалистами GlobalTrust была разработана программа и методика тестовых испытаний для Microsoft Dynamics NAV, направленных на выявление уязвимостей и несоответствий требованиям безопасности, выполнено проектирование общей архитектуры системы защиты, разработана проектная документация, внедрены дополнительные средства защиты информации.

По словам генерального директора GlobalTrust Александра Астахова: *«Ключевыми особенностями Microsoft Dynamics NAV как объекта защиты являются ее распределенная клиент-серверная архитектура, многоуровневость, а также концентрация основного объема обрабатываемой информации в базе данных MSSQLServer. Уязвимости данной ERP-системы распределены по уровням, также как и ее функциональные компоненты: сетевой уровень, уровень операционной системы, уровень СУБД, прикладной уровень, веб-интерфейсы, клиентские компоненты ERP-системы. Для каждого из этих уровней характерен свой набор слабых мест, которые могут повлечь компрометацию всей системы, даже в случае идеально настроенных остальных. Отдельную проблему представляет достаточно сложная система управления доступом к объектам внутри ERP-системы. Поэтому для контроля распределения прав доступа могут потребоваться дополнительные специализированные средства, разрабатываемые для Microsoft Dynamics NAV».*

Результаты работы позволили выявить и устранить имеющиеся уязвимости и несоответствия в одной из ключевых бизнес-систем медиа холдинга и повысить защищенность обрабатываемых в Microsoft Dynamics NAV персональных данных и финансовой информации.

GlobalTrust оценил соответствие Тексбанка требованиям Положения Банка России № 382- П

написано GlobalTrust.ru | 24.07.2017



Эксперты GlobalTrust оценили соответствие Тексбанка требованиям Положения Банка России № 382-П по обеспечению защиты информации при осуществлении переводов денежных средств.

В ходе проведенного компанией GlobalTrust аудита процессов и систем денежных переводов АО АКБ «Тексбанк» было подтверждено соответствие требованиям Положения Банка России № 382-П от 09 июня 2012 (редакция от 14.08.2014) по обеспечению защиты информации при осуществлении переводов денежных средств.

Итоговый показатель соответствия Rпс для АО АКБ «Тексбанк» составил 0,77. Это означает, что работа в АО АКБ «Тексбанк» по обеспечению защиты информации при осуществлении переводов денежных средств, в целом, обеспечивает выполнение установленных требований. Значение качественной оценки выполнения требований – удовлетворительная.

Данный показатель соответствия улучшился по сравнению с результатами предыдущей оценки. В ходе проекта были выработаны рекомендации по совершенствованию механизмов защиты информации систем денежных переводов и сформирован план мероприятий по устранению выявленных недостатков.

В ходе выполнения работ были решены следующие задачи:

▪ **Оценка соответствия требованиям Положения Банка России № 382-П**

- Сбор и анализ свидетельств аудита
- Анализ документации, интервьюирование представителей организации
- Оценка выполнения требований категорий 1-3
- Вычисление обобщающих показателей соответствия EV1пс и EV2пс
- Вычисление итогового показателя соответствия Rpс
- Документирование результатов оценки соответствия требованиям 382-П
- Планирование мероприятий по обеспечению соответствия 382-П
- Подготовка и согласование отчетных документов

▪ **Разработка организационно-распорядительных документов для обеспечения соответствия требованиям 382-П**

- Проведение интервьюирования уполномоченного персонала Банка
- Анализ и документирование процессов и методов обеспечения ИБ
- Определение требований к процессам обеспечения ИБ
- Определение ролей и ответственности персонала, а также порядка взаимодействия между подразделениями
- Разработка и согласование проектов ОРД по обеспечению ИБ
- Доработка проектов ОРД, устранение замечаний

В ходе выполнения проекта специалистами GlobalTrust были подготовлены следующие документы:

- Отчет о соответствии 382-П
- План мероприятий по обеспечению соответствия требованиям 382-П
- Более 20 организационно-распорядительных документов, регламентирующих различные аспекты защиты информации в

платежных системах Банка.

Аудит безопасности и оценка рисков маркетингового агентства

написано GlobalTrust.ru | 24.07.2017



Аудит информационной безопасности, оценка и обработка информационных рисков одного из ведущих российских маркетинговых агентств.

В 2008 году компанией GlobalTrust был реализован проект по аудиту информационной безопасности, оценке и обработке информационных рисков одного из ведущих российских маркетинговых агентств, предоставляющего услуги крупнейшим российским компаниям, являющимся лидерами в своих сегментах рынка. Компания GlobalTrust была выбрана в качестве исполнителя работ по результатам закрытого тендера.

В ходе выполнения работ были успешно решены следующие задачи:

- Идентификация уязвимостей информационной безопасности в информационных системах и сетевой инфраструктуре Заказчика
- Идентификация каналов утечки конфиденциальной информации
- Идентификация и оценка рисков информационной безопасности
- Оценка надежности и полноты предпринимаемых Заказчиком мер по обеспечению информационной безопасности, соответствие этих мер внутренним стандартам организации, нормативной базе и передовому опыту

- Идентификация экономически обоснованных механизмов контроля информационной безопасности и мер по обработке информационных рисков

Для оценки информационных рисков специалистами GlobalTrust применялась собственная методология, доказавшая свою эффективность и 100% совместимость с требованиями международного стандарта ISO 27001.

Результаты данной работы позволили Заказчику спланировать мероприятия в области информационной безопасности таким образом, чтобы обеспечить экономически оправданный уровень безопасности, соответствие требованиям учредителей, клиентов и партнеров. Реализация данного плана позволит Заказчику в дальнейшем успешно пройти сертификационный аудит на соответствие ISO 27001.

Обследование информационных систем персональных данных туристической компании

написано GlobalTrust.ru | 24.07.2017



Обследование информационных систем персональных данных, разработка Концепции обеспечения безопасности персональных данных и Технического задания на проектирование системы защиты персональных данных

В 2010 году компания GlobalTrust выполнила проект по обследованию

информационных систем персональных данных известной российской туристической фирмы, осуществляющей как отправку российских граждан на отдых зарубеж, так и прием иностранных граждан в России.

Основной целью выполнения работ являлось обеспечение соответствия организации Заказчика требованиям Федерального Закона РФ № 152 «О персональных данных», а также требованиям, выпущенных на его основе подзаконных актов и нормативных документов регулирующих органов.

В ходе данного проекта специалистами GlobalTrust были выполнены следующие работы:

- Сбор и документирование исходных данных по ИСПДн, включая физическое расположение, организационную структуру, состав и структуру программно-технических средств, процессы обработки ПДн и т. п.
- Идентификация и анализ применимых требований законодательства и нормативной базы по ПДн, а также проверка их выполнения
- Определение перечней ПДн, способов их получения, обработки и защиты
- Идентификация и анализ существующих процессов и средств обеспечения безопасности ПДн
- Идентификация, документирование и классификация ИСПДн
- Разработка модели актуальных угроз в отношении ПДн и модели нарушителя
- Анализ защищенности ИСПДн, идентификация и анализ технических и организационных уязвимостей
- Разработка Концепции обеспечения безопасности ПДн
- Разработка Технического задания на создание СЗПДн

Результаты данной работы позволили Заказчику выявить существующие несоответствия требованиям законодательства в области персональных данных, идентифицировать слабые места в системе защиты персональных данных и разработать четкую программу действий по приведению своих ИСПДн в соответствие с ФЗ-152 и совершенствованию системы защиты персональных данных в соответствии с требованиями нормативно-методических документов ФСТЭК России.

Разработка системы защиты персональных данных для Mango Telecom

написано GlobalTrust.ru | 24.07.2017



Компания GlobalTrust сообщает о завершении проекта по разработке системы защиты персональных данных Манго Телеком – российского провайдера облачных коммуникационных сервисов.

Манго Телеком разрабатывает софт, предоставляет в аренду приложения (бизнес-модель SaaS) и оказывает услуги связи, работая на стыке ИТ и телекоммуникаций.

В ходе выполнения работ специалистами GlobalTrust решались следующие задачи:

- Обеспечение соответствия процессов обработки персональных данных Манго Телеком, требованиями 152-ФЗ «О персональных данных»
- Разработка системы защиты персональных данных в соответствии с Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными документами ФСТЭК и ФСБ России.

Работы включали в себя два этапа:

- Предпроектное обследование ИСПДн, определение уровня защищенности ПДн, разработку модели нарушителя и модели актуальных угроз ПДн, а также технического задания на создание СЗПДн
- Техническое проектирование СЗПДн и разработку организационно-распорядительных документов по обработке и защите персональных данных, включая: положения, планы, инструкции, приказы, акты, журналы, перечни, а также типовые формы обязательств, уведомлений и согласий субъектов на обработку ПДн

«Обработка и защита персональных данных у телекоммуникационных операторов имеет свою специфику. Этим в частности обусловлена разработка отраслевого стандарта защиты персональных данных «большой тройкой» операторов сотовой связи. Дополнительные трудности для ряда операторов связаны с вступлением в силу с 1 сентября 2015 года 242-ФЗ, обязывающего использовать при сборе ПДн базы данных, находящиеся на территории РФ. Только начинает формироваться практика регулирования вопросов обработки и защиты персональных данных в «облаках». Новый международный стандарт ISO/IEC 27018:2014 — Практическое руководство по защите персональных данных, обрабатываемых в публичных облаках, — первый шаг в этом направлении. Все эти вопросы должны быть увязаны с требованиями российских регуляторов: ФСТЭК, ФСБ и Роскомнадзора», — отметил Александр Астахов, генеральный директор GlobalTrust.