Одна из самых популярных соцсетей для врачей с широкими возможностями для фармацевтических брендов — «Доктор на работе». Сетью заявлено 545400 зарегистрированных пользователей - врачей. С «Доктор на работе» активно сотрудничают крупные фармкомпании: Pfizer, Servier, Bayer, Astellas, Sanofi и многие другие.

Все соцсети для врачей при регистрации требуют предоставление подробной информации о медицинском образовании и специализации врача, чтобы сделать сообщество максимально закрытым в профессиональном плане.

Пока не очень распространены, но набирают популярность специальные мобильные приложения для врачей с широким функционалом: от подробной интерактивной информации о препаратах, календаря записи пациентов до различных возможностей диагностики. Например, приложения «Мир врача» и «Мобильный врач».

Список литературы / References

1. Исследование JagaJam «Присутствие фармацевтических брендов в социальных сетях», 2015. [Электронный ресурс]. Режим доступа: http://www.jagajam.com/data/presentation/pharma_brands_in_socialmedia.pdf/ (дата обращения: 06.06.2018).
2. Исследование Ipsos Healthcare «Digital - каналы и технологии в продвижении продуктов на фармацевтическом рынке и трансформация коммуникаций с врачебным сообществом» [Электронный ресурс]. Режим доступа: https://www.ipsos.com/ipsos-comcon/ru-ru/vrema-digital/ (дата обращения: 10.06.2018).
3. Исследование портала Evrika.ru «Значение социальных сетей для врачей» [Электронный ресурс]. Режим доступа: https://www.evrika.ru/show/1395/ (дата обращения: 06.06.2018).

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ АКТИВОВ ПРЕДПРИЯТИЯ

Глухов Н.И.[1], Непомнящих И.А.[2] Email: Glukhov643@scientifictext.ru

[1]Глухов Николай Иванович - кандидат экономических наук;
[2]Непомнящих Иван Александрович – магистрант,
кафедра информационных систем и защиты информации,
Иркутский государственный университет путей сообщения,
г. Иркутск

Аннотация: *в данной статье проанализирована информационная система управления инцидентами «Octopus» предприятия «ЛАН АТМсервис», в которой вся информация обрабатывается в едином информационном потоке, то есть существует проблема разграничения доступа, так же проанализирована локальная нормативна база. На основе анализа, выявлены особенности информационной системы, установлено отсутствие локальных нормативных документов по защите информации, выявлены уязвимости. Так же описаны правила защиты информации и представлены методы решения выявленных проблем.*

Ключевые слова: *информация, информационная безопасность, защита информации, информационные технологии, аудит, информационные активы предприятия, информационные ресурсы.*

PECULIARITIES OF PROTECTION OF COMPANY'S ASSETS

Glukhov N.I.[1], Nepomnyashchikh I.A.[2]

[1]Glukhov Nikolai Ivanovich - Candidate of economic sciences;
[2]Nepomnyashchikh Ivan Aleksandrovich – Master,
INFORMATION TECHNOLOGIES AND INFORMATION SECURITY,
IRKUTSK STATE UNIVERSITY OF RAILWAY TRANSPORT,
IRKUTSK

Abstract*: in this article, the incident management information system "Octopus" of the LAN ATMservice enterprise is analyzed, in which all information is processed in a single information flow, that is, there is a problem of access delimitation, as well as a local regulatory base. Based on the*

analysis, the features of the information system are revealed, the absence of local regulatory documents on the protection of information is revealed, vulnerabilities are revealed. Also, the rules for protecting information are described and methods for solving the identified problems are presented.
Keywords: *information, information security, information technology, enterprise information assets, information resources.*

УДК 004

Любая защита информации начинается с обследования информационной системы предприятия. В нашем случае таковой системой является система управления инцидентами Octopus. Система управления инцидентами Octopus позволяет клиентам «ЛАН АТМсервис» оперативно регистрировать свои обращения по обслуживанию банковского оборудования и контролировать ход выполнения каждого инцидента в режиме реального времени. Система Octopus имеет удобный и дружелюбный пользовательский WEB-интерфейс, посредством которого клиенты могут удаленно размещать обращения и отслеживать ход исполнения заявки. Интерфейс также служит удаленной консолью доступа в систему для партнеров и подрядчиков. Данный функционал позволяет сократить время обработки и маршрутизации обращений. Система Octopus разработана на базе платформы 1С: Предприятие 8. При регистрации обращения система обеспечивает контроль соответствия информации, предоставленной клиентом, действующему сервисному договору. Автоматическая проверка на повторность обращения позволяет детально изучить историю обслуживания конкретного оборудования и выбрать оптимальный вариант решения имеющейся проблемы.

Так же в единой информационной базе находятся:

- база клиентов,
- банковские и кассовые операции, клиент-банк, платежный календарь,
- расчеты с контрагентами, персоналом,
- учет материалов, товаров, продукции,
- заказы клиентов, заказы-наряды,
- учет выполнения работ и оказания услуг,
- учет производственных операций,
- учет персонала, расчет управленческой заработной платы,
- учет затрат и расчет себестоимости,
- имущество, капитал,
- доходы, расходы, прибыли и убытки
- финансовое планирование (бюджетирование) и т. д.

В программе предусмотрено оформление практически всех первичных документов торгового и производственного учета, а также документов движения денежных средств.

В программе реализовано все самое необходимое для ведения оперативного учета, контроля, анализа и планирования на предприятии. Решение не перегружено излишним функционалом, его можно легко настроить на особенности организации управления и учета в компании – это обеспечивает возможность "быстрого старта" и удобство ежедневной работы. Однако вопросов и проблем в области информационной безопасности еще достаточно в частности:

- отсутствует квалифицированный специалист, ответственный за информационную безопасность;
- отсутствуют правила безопасности и регламент реагирования на инциденты, связанные с информационной безопасностью (утечка конфиденциальной информации, кража паролей или их потеря, реакция на сетевые атаки и т.д.)
- в одной информационной системе невозможно содержать все данные с разными уровнями защиты;
- при трудоустройстве с сотрудниками, которые имеют доступ к клиентской базе, к CMS, к персональным данным клиентов и сотрудников не подписывается соглашение о конфиденциальности;
- не применяется парольная политика (требования к сложности пароля, контроль за сменой паролей, реагирование на компрометацию, назначение ответственного);
- не ведется учет носителей информации (таких как флешки, жесткие диски);
- отсутствуют регулярные антивирусные проверки компьютеров организации.

Особенность защиты информационных активов предприятия заключается в соблюдении основных правил [2]:

1. Все используемые средства для защиты должны быть доступными для пользователей и простыми для технического обслуживания.
2. Каждого пользователя нужно обеспечить минимальными привилегиями, необходимыми для выполнения конкретной работы.
3. Система защиты должна быть автономной.
4. Необходимо предусмотреть возможность отключения защитных механизмов в ситуациях, когда они являются помехой для выполнения работ.
5. Разработчики системы безопасности должны учитывать максимальную степень враждебности окружения, то есть предполагать самые наихудшие намерения со стороны злоумышленников и возможность обойти все защитные механизмы.

Наличие и месторасположение защитных механизмов должно быть конфиденциальной информацией.

Для решения поставленных задач и соблюдения предложенных правил требуется разделить информационную систему Octopus.

Требуется разделить на несколько информационных систем и разграничить доступ персонала к данным информационным системам:

1) Система клиентов:
- база клиентов
- заказы клиентов, заказы-наряды

2) Финансовая система
- банковские и кассовые операции, клиент-банк, платежный календарь
- расчеты с контрагентами, персоналом
- расчет управленческой заработной платы
- учет затрат и расчет себестоимости
- доходы, расходы, прибыли и убытки
- финансовое планирование (бюджетирование)

3) Система выполненных работ
- заказы клиентов, заказы-наряды
- учет выполнения работ и оказания услуг,
- учет производственных операций

4) Капитал
- имущество, капитал.

Также требуется:

Ввести еженедельные антивирусные проверки с помощью сертифицированного антивируса на всех АРМ компании.

Составить документы на учет внешних носителей и составить список ответственных лиц за выданные внешние носители [4].

Составить пакет документов для новых сотрудников об ответственности при раскрытие конфиденциальной информации.

Выделить рабочее место для специалиста по информационной безопасности.

Составить парольную политику.

В данной статье нами были проанализированы информационные ресурсы организации ООО «Лан АТМсервис». Обозначен ряд проблем, связанных с ненадлежащим выполнением задачи защиты информации, что может привести к серьезным потерям. Описаны особенности решения поставленных задач и предложены способы решения задач.

Список литературы / References

1. *Глухов Н.И.* «Оценка информационных рисков предприятия: учебное пособие». Иркутск. ИрГУПС, 2013. 148 с.
2. *Гладких А.А., Дементьев В.Е.* «Базовые принципы информационной безопасности вычислительных сетей». Ульяновск: УлГТУ, 2009. С. 156.
3. *Газизова Э.Р., Веденьев Л.Т.* «Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов», 2009. 552 с.
4. Федеральная служба по техническому и экспортному контролю. [Электронный ресурс]. Режим доступа: http://fstec.ru/ (дата обращения: 19.06.2018).