**Источники литературы**

1. Федоров, Д. Конфигуратор продукции как составная часть идеологии CSRP [Электронный ресурс] / Д. Федоров // САПР и графика. – 2005. – № 10. – Режим доступа: http://www.sapr.ru/article.aspx?id=14582&iid=692. – Дата доступа: 30.11.2016.
2. Системы управления жизненным циклом сложных объектов (PLM) [Электронный ресурс] // НТЦ «Конструктор». – Режим доступа: http://constructor.ru/solutions/967/. – Дата доступа: 30.11.2016.
3. Технологии PLM [Электронный ресурс] // Компания «КЭЛС-центр». – Режим доступа: http://www.calscenter.ru/technology/. – Дата доступа: 30.11.2016.

*Ждан Юлия Геннадьевна*
*Белорусский государственный экономический университет*

## Проблемы защиты информации при использовании Интернет-технологий в современном менеджменте

В период становления информационной экономики ведение бизнеса невозможно представить без использования глобальной сети. В нашу жизнь она вошла очень прочно и стала не просто развлечением, а необходимостью.

Интернет – достижение человечества, позволяющее добывать знания, находить нужную информацию, общаться с людьми разных национальностей, изучать языки, и все это не выходя из дома и офиса. Но мы, чаще всего, не задумываемся над тем, какой вред может нанести Интернет нашему компьютеру и хранящейся там информации.

С развитием Всемирной паутины одной из важнейших проблем стало обеспечение сохранности информации и данных, ведь благодаря повсеместному использованию современных информационно-коммуникационных технологий и активному их внедрению во все сферы жизнедеятельности человека с их помощью через глобальную сеть мы можем проводить даже финансовые операции (например, пополнять электронный кошелек, осуществлять банковские переводы, покупку товаров, производить оплату коммунальных услуг и т д.), а это требует повышенных мер безопасности. На сегодняшний день велика вероятность несанкционированного доступа к данным, искажения и удаления информации. После этого возникает вопрос: «Кто может получить конфиденциальную информацию и как?»

Следуя [1], это может быть хакер. Для него не составит труда взломать систему защиты сайта или портала и получить доступ к информации. Шантажист также может получить информацию к данным. Например, при регистрации на сайтах знакомств люди указывают личные данные (номер телефона, адрес почтового ящика). При этом не обращают внимания на тот факт, что по этим данным легко можно найти компромат. Также существуют группы людей, собирающие персональные данные (паспортные данные, контактные телефоны, адреса). В этом случае может быть замешан сотрудник портала, имеющий доступ к конфиденциальной информации. Пройдет некоторое время и беспечный пользователь узнает, возможно, даже и от представителей правоохранительных органов, что на него зарегистрирована оффшорная (или другая) компания. Представитель известных силовых структур может без труда получить доступ к личным данным. Ему достаточно вежливо попросить у администрации сайта нужную информацию.

Согласно [2], приведем примеры наиболее известных Интернет-преступлений с момента создания глобальной сети.

Когда Интернет еще назывался ARPANET, был совершен самый первый взлом. Данное событие произошло в 1983 году. Кевин Митник, один из первых хакеров, когда ему было 17 лет, получил доступ к главному компьютеру Пентагона. За что и был впервые арестован.

Летом 2005 года произошел самый крупный за всю историю взлом. Компания MasterCard International и компания Visa пострадали в результате хакерского взлома

процессингового центра компании CardSystems Solutions Inc, которая занималась обработкой платежей для фирм и банков. Для получения конфиденциальной информации, хакеры внедрили в систему вирус, в результате чего, получили информацию о более чем 40 млн. кредитных карт всех существующих типов и завладели почти 3 млн. $ США.

Летом 2010 года была задержана группа, состоящая из 12 человек. Они отмывали деньги посредством iTunes. Группировка занимались приобретением собственного контента с помощью украденных данных дебетовых и кредитных банковских карт. Организовав фирму, выкладывающую музыкальные композиции в Интернет-магазины Amazon и iTunes, они покупали свои же композиции. В результате фирма заработала за период с осени 2008 по 2010 год более 300 тыс. $.

Существует еще много примеров громких преступлений, связанных так или иначе с глобальной сетью, которые доказывают, что мы живем в современном мире, где проблемы защиты информации встают более остро.

Для хакеров одним из самых интересных и увлекательных занятий, которое дает простор для воображения, является взлом аккаунтов. Они используют вполне логичную схему. Для начала атакующий получает доступ к одному из компьютеров посредством письма, которое содержит вредоносный документ PDF или Word, – в результате пораженная машина станет слабым звеном в корпоративной сети. И уже отсюда хакер будет вести поиск других уязвимостей, чтобы прыгать из компьютера в компьютер в поисках ценных данных – таблиц, документов, финансовой информации и других нужных файлов.

Когда подобные данные найдены, наступает время «экспорта». Файлы должны быть где-то собраны, и обычно атакующий выбирает под склад один из пользовательских компьютеров в сети, а не сервер. По словам Райана Казанцияна и Шона из компании Mandiant [3], специализирующейся на безопасности, подобная тактика хакера обусловлена привычками пользователей – они обычно не следят, сколько на их компьютере свободного места, в то время как системный администратор может заметить, что на одном из серверов неожиданно прибавилось данных.

Некоторые хакеры собирают все данные на «складской» машине, а потом скачивают их в один прием. Но чаще атакующие загружают информацию понемногу – даже, несмотря на то, что риск обнаружения в таком случае выше. И хотя некоторые хакеры крадут только конкретные данные, многие другие воруют все, на что могут «наложить лапу» – это характерный признак большой операции, в которой предусмотрены людские ресурсы для анализа кучи награбленного в поисках ценностей.

Рассмотреть детально проблемы защиты информации непосредственно на предприятии. Как сказал Уинстон Черчилль: «Владеешь информацией – владеешь миром» [4]. Перечисление денег, оплата кредитов, переговоры с крупным клиентом – это малая толика важной информации, которая требует защиты уже сегодня. Некоторые руководители предприятий не видят необходимости в защите своих предприятий, объясняя это отсутствием важной информации. Но это далеко не правильное решение, так как каждый день на предприятии совершается множество различных денежных операций.

Примером того, как утечка информации оставила компанию без клиентов является случай произошедший в компании Hitsniffer, которая специализируется на веб-аналитике [5]: по версии руководства компании, один из программистов, работавший в компании с момента ее основания, получил доступ к клиентской базе (имена, электронные адреса и т.д.), после чего создал массовую рассылку писем, где предложил сотрудничество всем заказчикам Hitsniffer от имени другой компании. Руководство закрыло сайт, предупредив клиентов о недобросовестности конкурентов. Затем отменила в одностороннем порядке все клиентские подписки на свои услуги в системе PayPal, посчитав неправильным принимать деньги от клиентов в тот момент, когда бизнес фактически остановлен.

На сегодняшний день существуют разнообразные способы защиты информации в глобальной сети. Их условно можно подразделить на несколько категорий [6-12]:

– организационные средства складываются из организационно-технических и организационно-правовых. К первым относят подготовку помещений, где расположены компьютеры, прокладка кабельной системы и др. Ко вторым же относят национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия. У организационного способа защиты информации есть свои плюсы и минусы. К плюсам можно отнести то, что они решают разнообразные проблемы, просты в исполнении, быстро реагируют на нежелательные действия в сети, имеют безграничные возможности изменения и развития. К минусам же приписывают высокую зависимость от персональных факторов, в том числе от общего формирования работы в определенном подразделении. Примером организационных средств защиты является разработка должностных инструкций, проведение беседы с работниками, комплекс мер наказания и поощрения;

– физические средства защиты – это различные устройства, аппараты, механизмы, конструкции, которые создают преграду на пути движения злоумышленника. К примерам физических средств защиты можно отнести охранную сигнализацию и охранное телевидение, заборы вокруг объектов, усиленные двери, стены, потолки, решетки на окнах и т.д.;

– технические средства защиты это различные по роду механизмы (электронные, электромеханические и т.п.), которые решают задачи информационной защиты. Примером является защита помещения от прослушивания;

– законодательные – совокупность нормативно-правовых актов, которые корректируют деятельность людей, имеющих доступ к секретным сведениям и назначающих степень ответственности за потерю и похищение охраняемой информации.

Вместе с тем, предприятию в целом и каждому сотруднику в частности под силу предпринять меры по предотвращению несанкционированного доступа к информации, ее кражи, искажения и др. Приведем простые, но эффективные правила и рекомендации по работе с глобальной сетью [13]:

– наличие хорошей антивирусной программы. При этом необходимо, чтобы антивирус мог работать в системе мониторинга – это поможет выявлять опасность сразу при ее возникновении;

– следует соблюдать осторожность при использовании неизвестных ресурсов в Интернете. В настоящее время для заражения компьютера достаточно посетить веб-страницу.

– после скачивания файлов, архивов и т.п. через Интернет необходимо проверить их с помощью антивирусного программного обеспечения на наличие вредоносного кода;

– почтовые письма, полученные от неизвестных и сомнительных отправителей, также необходимо проверить надежной антивирусной программой, иначе в краткие сроки ваш компьютер может превратиться в рассадник вирусов;

– ни в коем случае нельзя отвечать на сообщения с просьбой прислать личные данные (логин, пароль и т.д.);

– если при посещении сайта требуется оставить личную информацию (ФИО, паспортные данные, пароли, адреса и т.д.), то она должна быть минимальной.

Важность Интернета для развития современного мира сложно переоценить, но не стоит забывать про элементарные способы защиты данных и информации. Стоит обезопасить себя и свой компьютер от чужих посягательств, ведь злоумышленники не спят, и будут отыскивать все новые способы атаки вашего компьютера. Для защиты информации, хранящейся на персональных компьютерах (ПК), стоит установить хорошую антивирусную программу. Следуя [14], приведем наиболее популярные антивирусные программы:

– **Advanced SystemCare Ultimate.** Часто возникает вопрос о замедлении работы ПК из-за антивирусной программы. Данный продукт обладает встроенными программами для оптимизации, чистки и ускорения ОС Windows. К тому же защищает компьютер от шпионов, троянских вирусов, опасных скриптов, а также обеспечивает безопасности при проведении финансовых операций посредством Интернета.

– **Антивирус Касперского.** Конечно же, на сегодняшний день это наиболее популярная антивирусная программа, о которой слышали почти все пользователи Всемирной паутины. Данный продукт довольно хорошо справляется со своей непосредственной работой, находит и устраняет большинство угроз. Количество продуктов довольно многообразно: начиная от установки обычного антивируса, заканчивая комплексной версией программы.

– **Dr.Web.** По популярности данная антивирусная программа не уступает Антивирусу Касперского. Сильной стороной этого продукта является обнаружение неизвестных вирусов. К тому же Dr.Web имеет такую замечательную утилиту, как Dr.Web Cureit. Благодаря ей можно проверить свой компьютер на разнообразные вирусы.

Каждый год антивирусное программное обеспечение совершенствуется, но, к сожалению, и количество компьютерных вирусов растет.

К тому же для обеспечения безопасности вашего ПК не достаточно антивирусных программ. Для того чтобы ваш компьютер не подхватил «инфекцию» стоит поменьше посещать сомнительные сайты, а также стараться проверять скаченные файлы перед запуском, если требуется оставлять личную информацию, то стоит ее ограничить.

По мнению Билла Гейтса [15]: «Если вас нет в Интернете – вас нет в бизнесе…». И это правда, главное не забывать про безопасность.

Рассмотренные в работе способы защиты информации от несанкционированного доступа и искажения могут быть использованы на предприятиях различных форм собственности и в повседневной жизни.

**Источники литературы**


1. Гладкий, А. Безопасность и анонимность работы в интернет / А. Гладкий// М. – 260 с.
2. Громкие Интернет-преступления [Электронный ресурс]. – Режим доступа : http://1webcent.ru/desjatka-gromkih-internet-prestupleniy. – Загл. с экрана. – Дата доступа: 12.12.2016.
3. Как хакеры крадут информацию? [Электронный ресурс]. – Режим доступа : https://blog.kaspersky.ru/kak-atakuyushhie-kradut-vashi-dannye/342. – Загл. с экрана. - Дата доступа: 12.12.2016.
4. Спе́нсер-Че́рчилль, Сэр Уи́нстон Леона́рд [Электронный ресурс]. – Режим доступа : http://cyclowiki.org/wiki/. – Загл. с экрана. - Дата доступа: 12.12.2016.
5. Пример кражи информации [Электронный ресурс]. – Режим доступа : https://www.anti-malware.ru/news/2016-09-12/2092. – Загл. с экрана. - Дата доступа: 12.12.2016.
6. Классификация средств защиты информационных систем [Электронный ресурс]. – Режим доступа : http://cyclowiki.org/wiki. - Загл. с экрана.- Дата доступа: 12.12.2016.
7. Организационные средства защиты информации [Электронный ресурс]. – Режим доступа : http://cyclowiki.org/wiki/. – Загл. с экрана. - Дата доступа: 12.12.2016.
8. Физические способы защиты [Электронный ресурс]. – Режим доступа : http://ru.bmstu.wiki. – Загл. с экрана. - Дата доступа: 12.12.2016.
9. Технические средства защиты [Электронный ресурс]. – Режим доступа : http://detektor.ru/prod/common/protect. – Загл. с экрана.- Дата доступа: 12.12.2016.
10. Законодательные средства защиты информации [Электронный ресурс]. – Режим доступа : http://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi. – Загл. с экрана. - Дата доступа: 12.12.2016.
11. Способы защиты информации [Электронный ресурс]. – Режим доступа : http://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi. – Загл. с экрана. - Дата доступа: 12.12.2016.
12. Основные проблемы защиты информации [Электронный ресурс]. – Режим доступа : http://ab-solut.net/ru/articles/problemi_zashiti. – Загл. с экрана.- Дата доступа: 12.12.2016.

13. Физические средства защиты информации [Электронный ресурс]. – Режим доступа : http://ru.bmstu.wiki. – Загл. с экрана. - Дата доступа: 12.12.2016.

14. Антивирусные программы [Электронный ресурс]. – Режим доступа : http://pcpro100.info/luchshie-antivirusyi-2016. – Загл. с экрана. - Дата доступа: 12.12.2016.

15. Гейтс, Билл [Электронный ресурс]. – Режим доступа : http://cyclowiki.org/wiki/. – Загл. с экрана. - Дата доступа: 12.12.2016.

*Каптыш Полина Евгеньевна*
*Белорусский государственный экономический университет*

## Сценарий кодификации как инструмент повышения эффективности консультационной поддержки пользователей (на примете ИТ-компании)

Одной из последних тенденций развития компаний является не только внедрение информационных технологий, но и активное использование знаний. Ставка делается на носителей знаний – работников, специалистов, менеджеров. Поэтому всё большее распространение получают технологии, основанные на применении знаний. Именно этим и обосновывается актуальность данной работы.

В условиях конкурентной борьбы уровень спроса на какую-либо продукцию при прочих равных обстоятельствах определяется не только потребительскими качествами товара, но и комплексом необходимых дополнительных услуг, оказываемых потребителю (сервисом).

Рассматриваемая в данной статье ИТ-компания является официальным партнером российской фирмы «1С», которая специализируется на разработке, дистрибьюции, издании и поддержке компьютерных программ делового назначения.

Для программных продуктов «1С: Предприятие» в рассматриваемой нами компании предусмотрено сервисное обслуживание по линии информационно-технологического сопровождения (ИТС), которое включает в себя:

– курсы в Центре Сертифицированного Обучения фирмы «1С»;

– обновление программного продукта – получение новых релизов программы и конфигураций, получение новых форм отчетности;

– услуги линии консультаций по телефону и электронной почте;

– поддержка пользователей через Интернет;

– ежемесячное получение комплекта дисков ИТС, содержащего технологические и информационные материалы, необходимые для эксплуатации системы, а также консультации, нормативные документы и справочники по бухгалтерскому учету и налогообложению, другие материалы;

– консультации в офисе – при желании клиента или в сложных ситуациях специалисты линии консультаций могут проконсультировать пользователя в офисе компании, при необходимости привлекая технических специалистов и разработчиков.

Остановимся подробнее на работе линии консультаций, сотрудники которой регулярно взаимодействуют с клиентами компании. Каждый сотрудник линии консультаций является ответственным за качественное выполнение услуг по оказанию помощи и проведению консультаций пользователям программных продуктов «1С».

К бизнес-процессам линии консультаций относятся: бизнес-процесс консультации по телефону; бизнес-процесс записи обновления; помощь в выборе программного обеспечения; консультация через Интернет. Бизнес-процесс консультации по телефону является основным в работе линии консультаций и состоит из следующих этапов:

1) Прием входящего звонка. При этом сотрудник узнает: