водителя.

Однако несмотря на высокий уровень достигнутых разработок, у кластера наблюдается явный разрыв между высоким качеством инновационной продукции и низким объемом ее реализации на рынке. Во многом это объясняется тем, что рынок инновационной продукции радикальным образом отличается от традиционного, и к нему не применимы методы классического маркетинга. В связи с этим кластеру важно уделить особое внимание налаживанию сбыта своей продукции, в частности, как созданию собственного технологического брокера, так и сотрудничеству со сторонними центрами трансфера технологий.

Заключение. Таким образом, для развития инновационных кластеров в России характерны две большие проблемы – небольшая доля частного финансирования и разрыв между высоким качеством инновационной продукции и низким объемом ее реализации на рынке.

Решение проблемы увеличения доли частного финансирования возможно

во-первых, в установлении особых льготных налоговых режимов для инновационных кластеров, а во-вторых, в создании инфраструктуры для привлечения частного капитала, в том числе иностранного. Проблема сбыта инновационной продукции может быть решена как через стимулирование сбыта посредством государственного заказа, так и с помощью специализированных компаний, занимающихся маркетингом инновационной продукции – технологических брокеров и центров трансфера технологий.

Список литературы

1. Портер М., 2005, Конкуренция. : Пер. с англ. – М.: Издательский дом «Вильямс».
2. Устинова Л.Н. Особенности развития промышленности в условиях цифровизации./ Монография «Формирование цифровой экономики и промышленности. Новые вызовы.Глава 3 /под редакцией д.э.н, проф. Бабкина.-СПб 2018, с.176-197.
3. Обзор инновационных кластеров в иностранных государствах. Миэкономразвития России. Май 2011г.
4. Клейнер Г., Бабкин А. формирование телекоммуникационного кластера на основе виртуального предприятия //конспекты лекций по информатике (включая подсерии конспект лекций по искусственному интеллекту и конспект лекций по биоинформатике). Т. 9247. 2015. С. 567-572.
5. Устинова Л.Н. «Индустрия 4 –новые вызовы для российского производства» / коллективная Монография по материалам научно-практической конференции «Цифровая экономика и ИНДУСТРИЯ 4» разд.1, Стр.81-87. 2018.

ОБЕСПЕЧЕНИЯ НОВОГО РЕСУРСА «ИНФОРМАЦИЯ» НА ПРЕДПРИЯТИИ

Гулид Анатолий Константинович
Тестировщик-Технический писатель, аэропорт Домодедово

Аннотация: *в данной статье рассматривается понятия как информация, информационная безопасность в компании, основные угрозы от мошенников и основные рекомендации к защите информации.*

Ключевые слова: *информация, угроза, информационная безопасность, информационные технологии, предприятие.*

Abstract: *this article discusses the concepts of information, information se-curity in the company, the main threats from fraudsters and the main recommen-dations for the protection of information*

Keywords: *information, threat, information security, information technolo-gies, enterprise.*

Введение. В век цифровых технологий, который развивается достаточно быстро, Информация всегда играла чрезвычайно важную роль в жизни человека. Вспоминается простая фраза «Тот, кто владеет информацией, тот владеет и миром». Следует отметить, что исключительная роль информации в современном мире привела к пониманию информации как ресурса, столь же необходимого и важного, как энергетические, сырьевые, финансовые и другие ресурсы. Информация стала предметом купли - продажи, т.е. информационным продуктом, который наравне с информацией, составляющей общественное достояние, образует информационный ресурс общества. В результате научно-технического прогресса человечество создавало все новые средства и способы сбора, хранения, передачи информации. Но важнейшее в информационных процессах является обеспечение защиты информации. Почти везде можно услышать простое понятие, которое связано с защитой

информации – «Информационная безопасность». Информационная безопасность создает условия формирования безопасного состояния информации и ее использование. Самый простой и очевидный пример – это мобильные телефоны, а точнее обеспечение защиты информации, которая хранится на телефоне, где самый простой пример защиты – это пароль. Многие не задумываются о полной защите и используют свою технику без паролей, что делает их технику уязвимой. В последнее время стало популярным использовать вместо паролей сканер отпечатков пальца или «Face ID»- сканирование лица, что не требуют в настройке большого времени[1].

В банках, например хранится вся информация об клиентах, потеря информация или простая утечка информации может помочь злоумышленникам получить все, что они хотят: начиная от фамилии клиента и заканчивая местом жительства, а более опытные злоумышленники могут получить не только эту информацию, но и доступ к вашим картам – деньгам.

Цель исследования: Аналитический анализ обеспечения безопасности персональных данных на предприятии.

Задачи исследования:

Проанализировать структуру информационной безопасности.

Рассмотреть законодательную базу по защите персональных данных.

Почти каждое предприятие располагает различными видами информации, представляющими интерес для злоумышленников. Прежде всего, это коммерческие данные, информация, являющаяся интеллектуальной собственностью предприятия и конфиденциальные данные. В стабильной компании, защита своих информационных систем, создает надежные и безопасные условия для работы. Утечки, отсутствие и кражи информации всегда влияет на состояние компании.

На данный момент есть три основных момента, которые должна соблюдать информационная безопасность[2]:

- целостность данных – обеспечение защиты достоверности и целостности информации

- доступность для пользователя – каждый вид информации должен быть открыт для чтения определенному кругу сотрудников. Тут стоит понимать, что из-за большого вида информации, которая хранится в компании, нужно строго понимать границы доступа.

- обеспечение недопустимости угроз повреждения и утраты информации - защиту непосредственно от угроз целенаправленного уничтожения или повреждения информации

Существует два основных вида угроз для информации

Первый вид угроз связан с хакерами и атаками вирусов. Данный вид угроз нацелен на кражу или порчу информации, что может привести к частичной или даже к полной потере информации. Такое действие может привести к частичной или полной остановке работы на предприятия с дальнейшими последствиями или убытками.

Второй вид угроз – это сотрудники предприятия. Тут можно выделить два типа деятельности по потери информации. Первый зависит от сотрудника, который обеспечивает саму информационную безопасность. Он должен своевременно обновлять программное обеспечение для защиты информации, производить резервное копирование для восстановления и следить за самим оборудованием, на котором хранятся все виды информации. С помощью определенных программ сотрудник информационной безопасности и обеспечивает доступ к нужной информации, которую использует пользователь, но и обеспечивает

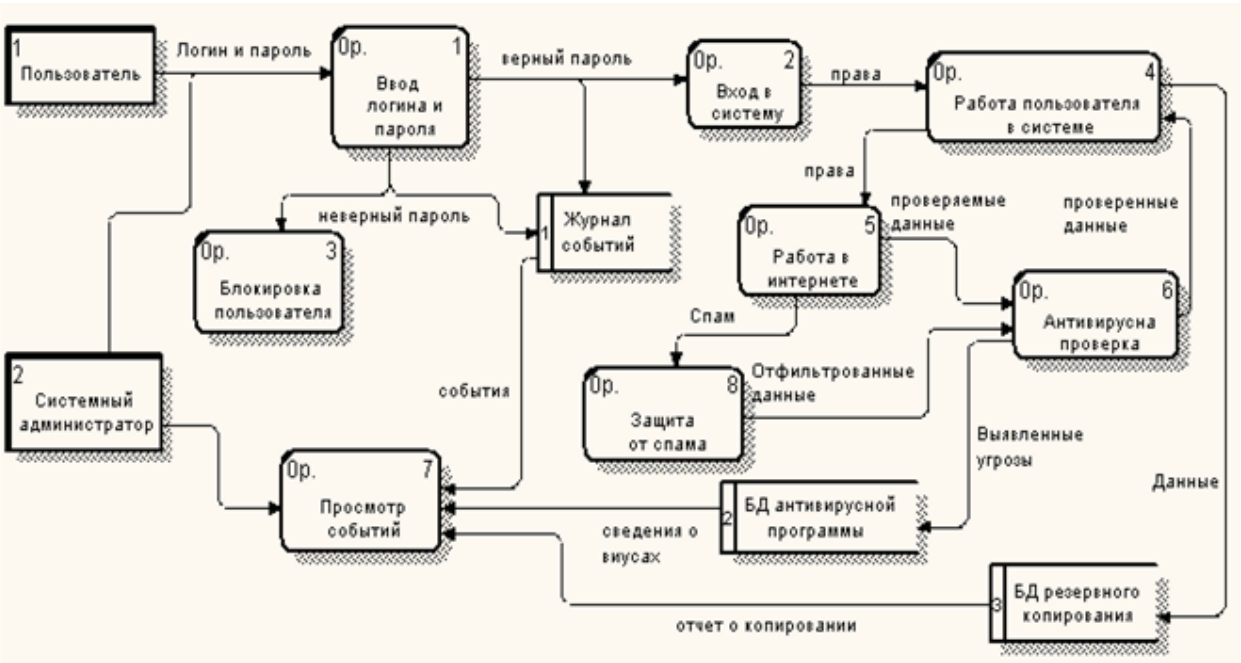

Рисунок 1. Структура информационной безопасности

защиту предоставляемой информации. На Рисунке 1 можно увидеть последовательность действий простого пользователя предприятия, где нужно учитывать доступ и безопасность информации.

Второй тип - это недовольные сотрудники, сотрудники «Шпионы», которые могут предоставить информацию третьим лицам, что может создать не мало проблем для предприятия. Тут уже влияет человеческий фактор. Для устройства на работу многие предприятия, для нового сотрудника, проводят множество мероприятий, которые помогают понять, что за человек к ним устраивается. Это может быть обычная беседа с психологом или даже прохождение полиграфа, что сразу показывает настрой и важность самого предприятия[4].

Переходя к рассмотрению вопросов защиты персональных данных, следует отметить, что они остаются неизменно острыми на протяжении последних лет и поднимаются в самых высоких кабинетах как в России, так и за рубежом, поскольку касаются каждого из нас, вне зависимости от гражданства и должности. С приходом информационных технологий защита личных данных стала еще более актуальной. В Федеральный Закон вносились изменения, основные из которых были введены 261-ФЗ от 25.07.2011 и 242-ФЗ от 21.07.2014. Первый закон внес существенные изменения в базовые постулаты защиты ПДн, а второй запретил первичную обработку ПДн за пределами территории РФ.

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. законы, которые относятся к сфере информационной безопасности[3]:

- Федеральный закон №152 «О персональных данных». ФЗ регулирует отношения между органами государственной власти во время поиска важных сведений и обеспечивает информационную безопасность персональных дан-ных

- Федеральный закон №63 «Об электронной цифровой подписи». ФЗ перечисляет области деятельности, в которых используется электронная циф-ровая подпись в целях обеспечения информационной безопасности. Напри-мер, покупка товаров, оказание услуг и т.д.

Федеральный закон «Об информации, информационных технологиях и о защите информации» был принят Государственной Думой 8 июля 2006 го-да, а одобрен Советом Федерации спустя 6 дней того же года. Последние из-менения были внесены 27 июля 2017 года.Государство также определят меру ответственности за нарушение положений законодательства в сфере ИБ. Например, глава 28 «Преступления в сфере компьютерной информации» в Уголовном кодексе Российской Федерации, включает три статьи:

- статья 272 «Неправомерный доступ к компьютерной информации»;

- статья 273 «Создание, использование и распространение вредоносных компьютерных программ»;

- статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»

Вывод: Информация в настоящее время приобрела коммерческую ценность, стала продуктом и товаром, которая важна для успешного развития предприятия, поэтому она нуждается в защите. Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного ПО и прочие угрозы приобретают более изощренный характер и набирают огромный темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить данные как маленького так и большого предприятия.

Список литературы

1. Алехина Г.В. Информационные технологии в экономике и управлении / Московский международный институт эконометрики, информатики, финансов и права. - М.: 2014. - 238 с.
2. Буга В.Д. Информационная безопасность на предприятии: что ей угрожает? средства защиты в сфере информационных технологий: какой антивирус наиболее эффективен // Молодежный научный форум: Технические и математические науки: электр. сб. ст. по мат. XI междунар. студ. науч.-практ. конф. №4.
3. Федеральный закон «О персональных данных» N 152-ФЗ от 27.07.2006 (ред. от 31.12.2017) // URL: http://www.consultant.ru/document/cons_doc_LAW_61801/
4. Драга А.А. Обеспечение безопасности предпринимательской деятельности. – М.: Издательство МГТУ им. Н. Э. Баумана. 2014. – 304 с.