РОССИЙСКИЙ МЕНЕДЖМЕНТ: СОВРЕМЕННЫЙ РАКУРС

Международный научно-практический журнал «Вестник МИРБИС» ISSN 2411-5703 http://journal-mirbis.ru/
№ 4 (20)' 2019, DOI: 10.25634/MIRBIS.2019.4
Ссылка для цитирования: Акинфеева Е. В. Информационная безопасность как фактор эффективной деятельности компании [Электронный ресурс] // Вестник МИРБИС. 2019. № 4 (20). С. 79–88. DOI: 10.25634/MIRBIS.2019.4.9.
Дата поступления 23.09.2019 г.

УДК 334.025

Екатерина Акинфеева[1]

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР ЭФФЕКТИВНОЙ ДЕЯТЕЛЬНОСТИ КОМПАНИИ

Аннотация. Актуальность исследования обусловлена тем, что слабая информационная безопасность способна привести не только к экономическим, финансовым и прочим потерям, но и поставить под угрозу все существование бизнеса. Поэтому необходимо учитывать при разработке стратегии компании/фирмы вопросы и проблемы, связанные с информационной безопасностью, и уделять им повышенное внимание. В связи с этим, данная статья направлена на анализ основных вопросов и проблем, связанных с утечкой информации компании.

В статье дан краткий анализ сложившейся ситуации, связанной с информационной безопасностью компании, ее защитой и сохранением. Представлены общие статистические данные по утечке информации, по основным российским структурам, компаниям и организациям, наиболее подверженным утечке информации. Показан размер ущерба, полученный российскими компаниями за 2017–2018 гг. и меры, принимаемые компаниями для своей защиты.

Материалы статьи представляют практическую ценность для фирм/компаний по предупреждению инцидентов, связанных с существующими угрозами утечки информации.

Ключевые слова: информация, конфиденциальная информация, кибератака, хакеры, утечка данных компании, размер ущерба, защита данных, стратегия компании.

JEL: M15

1 **Акинфеева Екатерина Владимировна** — кандидат экономических наук, доцент, ведущий научный сотрудник, Федеральное государственное бюджетное учреждение науки Центральный экономико-математический институт РАН (ЦЭМИ РАН). Москва, Россия. E-mail: katerina@cemi.rssi.ru.
AuthorID: 256280

Введение

Важную роль в развитии экономики играют как предприятия, ориентированные на промышленное производство, так и компании/фирмы быстро окупающегося не промышленного бизнеса. Эти организационные структуры не промышленного бизнеса способны не только создавать рабочие места, остро реагировать на появление разнообразных новшеств, гибко приспосабливаться к изменениям конъюнктуры рынков, но и быть источниками разработок, внедрения в производство и вывода на рынок новых товаров, услуг, технологий.

Стратегия развития любой компании/фирмы направлена как на разработку ее целей развития и функционирования, повышения устойчивости ее финансового положения и конкурентоспособности, на получение долгосрочной прибыли, приспособление к существующим рыночным условиям, так и на удовлетворение потребностей потребителя. В большинстве случаев для достижения этих целей компании/фирме необходима внутренняя реструктуризация, направленная на создание новых подразделений в самой структуре. Но без современных автоматизированных информационных систем как внутреннее, так и внешнее взаимодействие в настоящее время невозможно, и это в свою очередь приводит к необходимости применения новых информационных технологий [Балановская, 2015].

Как известно, информация для любой организационной структуры является особой ценностью и ее утечка или разглашение способны привести к необратимым последствиям. Один из ключевых вопросов, на который должна отвечать каждая теории фирмы — определение границ фирмы в пространстве, а также уровень проницаемости этих границ. В эпоху стремительного развития информационно-коммуникационных технологий проблема сохранения конфиденциальной информации затрагивает все стороны функционирования фирмы (компании, пред-

приятия). Если традиционные варианты теории фирмы рассматривают исключительно физические границы предприятия в экономическом пространстве, то с позиции междисциплинарной теории фирмы [Рыбачук, 2018; Клейнер, Рыбачук, 2019] предприятие имеет, в том числе, и информационные границы, что является весьма важным для его деятельности. Задача обеспечения информационной безопасности фирмы является междисциплинарной и не может быть решена силами одной дисциплины.

В данной работе, выполненной при поддержке Российского фонда фундаментальных исследований (проект № 17-02-00513-ОГН) развивается междисциплинарная теория фирмы в части исследования информационных границ предприятия, обеспечения их целостности, анализа возможных утечек информации и поиска мер противодействия им. Проводится оценка ситуации, сложившейся в настоящий момент в области информационной безопасности предприятий, а также рассматриваются вопросы, связанные с сохранением и защитой данной информации.

Под информацией принято понимать любые сведения, данные, которые принимаются и передаются, а также сохраняются различными источниками. Под конфиденциальной информацией понимается секретная информация, не подлежащая огласке.

На данный момент в российском законодательстве чёткого определения понятия «конфиденциальная информация» нет. В утратившем силу ФЗ РФ № 24 записано, что «конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации[1]».

В действующем ФЗ РФ N 149-ФЗ «Об информации, информационных технологиях и защите информации» определено понятие «конфиденциальности». Так, «конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя». Согласно этому же закону «информация — сведения (сообщения, данные) независимо от формы их представления[2]» [Васильев, Портнов, 2015].

В различных странах понятия конфиденциальность и информация, относящаяся к конфиденциальной, определяются по-разному. Так, в странах Европейского союза конфиденциальность информации регулируется с помощью ряда соглашений и директив, таких как директива ЕС 95/46/EC, 2002/58/EC и ETS 108, ETS 181, ETS 185, ETS 189. Например, конвенция «О преступности в сфере компьютерной информации» (ETS N 185) направлена на сдерживание, в том числе, действий, направленных против конфиденциальности компьютерных данных и компьютерных сетей, систем. Согласно данной конвенции для противодействия преступлениям против конфиденциальности, доступности и целостности компьютерных данных и систем каждая страна принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно её внутригосударственному праву:

- противозаконный доступ;
- неправомерный перехват;
- воздействие на данные;
- воздействие на функционирование системы.

Противозаконное использование устройств[3].

Наиболее сложно регулируемый вопрос — это конфиденциальность информации в Интернете. Это объясняется тем, что сохранность данных зависит в основном от субъекта (не важно, физического или юридического лица), от того, как, какую и в каком количестве информацию он предоставляет. Так, например, при посещении сайта, настройке учетной записи, совершении покупок через Интернет, регистрации, принятии участия в опросах, загрузке программного обеспечения собирается личная информация. Конфиденциальность в этой области регулируется в основном политикой конфиденциальности, которая прописывается на сайтах компаний.

Очевидно, что информация является стратегически важным товаром и соответственно потеря информации, завладение секретной информацией конкурентами является губительным для компании, наносящим не только ущерб, но и способным привести к ее банкротству [Максимов, Сонников, 2000].

Под утечкой информации российская компания InfoWatch, специализирующаяся на информационной безопасности в корпоративном секторе, понимает намеренные или случайные действия

1 Федеральный закон от 20 февраля 1995г. №- 24 ФЗ «Об информации, информатизации и защите информации» // СПС КонсультантПлюс.

2 Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС КонсультантПлюс.

3 Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001г.) // Гарант. URL: https://base.garant.ru/4089723/#friends (дата обращ. 29.08.2019 г.).

(как внешних злоумышленников, так и внутренних нарушителей), в результате которых нарушена конфиденциальность данных[4].

Число зарегистрированных утечек данных из компаний и организаций в 2018 г. выросло более чем на 5 % по сравнению с 2017 г. Более половины всех случаев зафиксированы в банковском и финансовом секторе, в высокотехнологичных компаниях, государственном секторе. За 2017–2018 гг. произошел существенный рост доли утечек информации в результате действий внутренних нарушителей и снижение доли инцидентов, совершенных через сетевой канал[5]. Наиболее крупные утечки информации, которые произошли в ряде стран, включая Россию, за 2018 г. показаны в таблице 1.

Таблица 1. **Статистика утечки информации (2018 г.)**

Страна	Структура	Финансовые потери
Индия	системы AADHAAR государственное хранилище идентификационных данных в мире	1 млрд долл.
Китай	логистическая компания SF Express	300 млн долл.
Россия	ИТ-компании VNG	около 163 млн долл.
Россия	Рособрнадзор	14 млн записей
США	гостиничная сеть Marriott (штаб-квартира находится в США)	100 млн долл.+500 млн записей
США	маркетинговая фирма Exactis	340 млн долл.
США	сервисный стартап Apollo	200 млн долл.
США	приложения Under Armour	150 млн долл.
США	социальная сеть Facebook	87 млн записей
Швейцария	разработчик ПО Veeam (штаб-квартира компании находится в Швейцарии)	440 млн. долл.

Источник: таблица составлена автором по данным: Главные утечки информации 2018 года // ItWeek, 27.12.2018. [WWW документ]. URL https://www.itweek.ru/security/news-company/detail.php?ID=204871 (дата обращения 29.08.2019).

Стоит отметить, что наиболее известная и скандальная утечка данных произошла именно в социальной сети Facebook. Личная информация (87 млн пользователей), которая была собрана в научных целях, была передана компании Cambridge Analytica.

В России в 2018 г. зарегистрировано 270 случаев утечки конфиденциальной информации из коммерческих и некоммерческих компаний, а также государственных структур и организаций. Если в 2017 г. в результате хакерских атак в России произошло 21,3 % зарегистрированных утечек, то по итогам 2018 г. эта доля сократилась до 9,5 %. Примерно 39 % инцидентов в результате хакерских атак пришлись на государственные и муниципальные организации[6].

В качестве основных причин утечки информации можно выделить следующие.

- Уязвимость сайта
- Вина руководства компаний
- Результат умышленных действий сотрудников компаний и организаций
- Использование служебной информации в мошеннических целях
- Превышение прав доступа к хранилищу данных
- Низкий уровень культуры информационной безопасности
- Наличие или хранение информации на бумажных или съемных носителях (около 45 % и около 43 %).

В общемировом распределении доля «российских» утечек составила 12 %. Объем скомпрометированных персональных данных, который пришелся на российские компании и государственные организации, не превысил 1 % от совокупного объема данных, скомпрометированных по всему миру [Годырева, 2008].

Основной проблемой для компаний и организаций остается внутренний нарушитель [7,8] [Дорофеев, Марков, 2014].

По статистике к основным российским структурам, компаниям и организациям, наиболее подверженным утечки информации следует отнести следующие (см. рисунок1).

- Банковский и финансовый сектор
- Высокотехнологичный сектор
- Промышленность и транспорт

4 Интернет-источник. Официальный сайт InfoWatch https://www.infowatch.ru/, посл. обращ. 29.08.2019 г.

5 Интернет-источник. Официальный сайт itweek. Главные утечки информации 2018 года. https://www.itweek.ru/security/news-company/detail.php?ID=204871, посл. обращ. 29.08.2019 г.

6 Там же.

7 Там же.

8 По данным экспертного центра по вопросам автоматизации государства и бизнеса в России TAdviser: официальный сайт. URL http://www.tadviser.ru/index.php.

- Государственный сектор и местные органы власти
- Сфера торговли и развлечений
- Медицинский сектор[1] [Волокитин и др., 2002].

1 Там же.

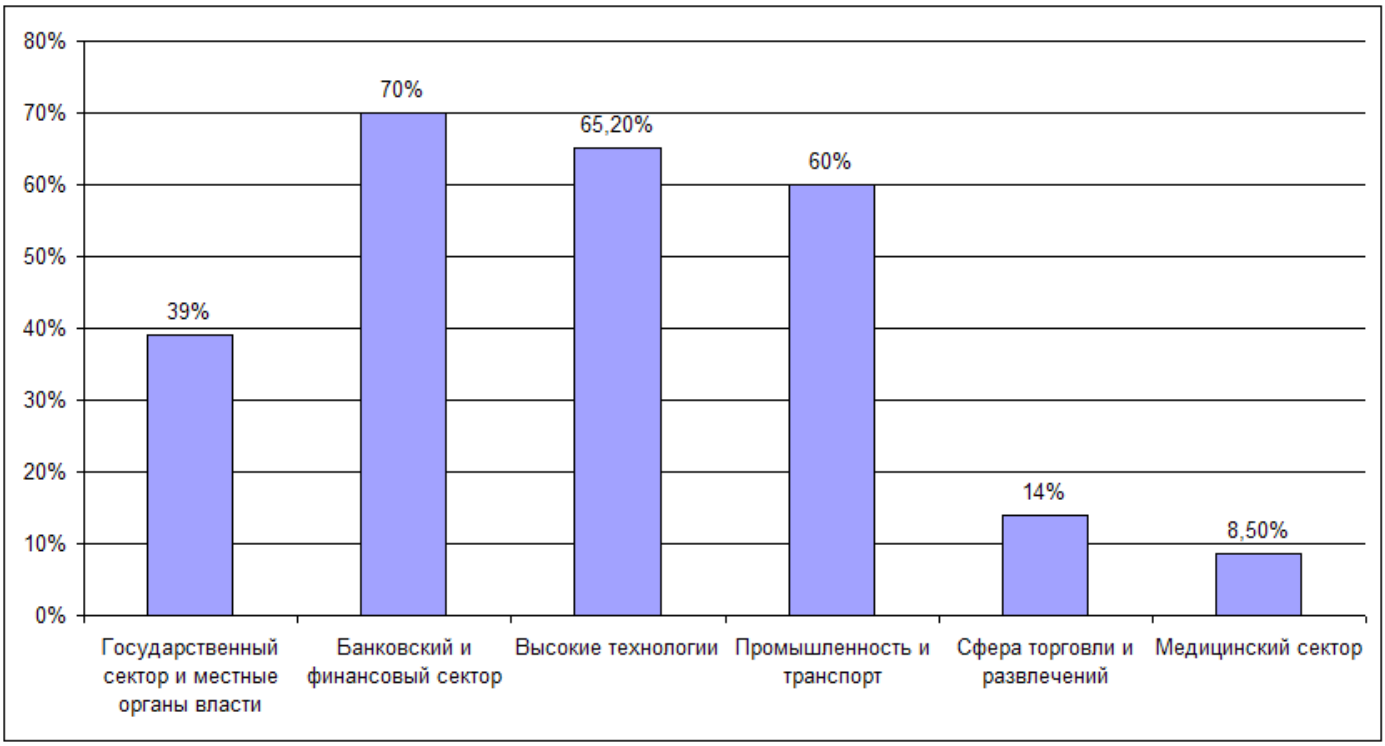

Рис. 1. Доля российских структур, компаний и организаций подверженных утечки информации
Источник: рисунок автора по данным официального сайта TAdviser, URL http://www.tadviser.ru/index.php

Стоит отметить, что сравнительно небольшая доля утечки информации в медицинском секторе объясняется тем, что в России пока еще низкий уровень цифровизации, как в медицинских учреждениях, так и в медицинском страховании. С одной стороны, отсутствие должного сетевого взаимодействия негативно отражается как на отрасли в целом, так и на пациентах, с другой стороны, таким образом, сохраняется безопасность персональных данных пациентов.

В финансовом и банковском секторах более подвержены утечки информации не крупные банки, которые обладают высокой технической оснащенностью, позволяющей выявлять и быстро реагировать на хакерские атаки, а небольшие банки. Это объясняется тем, что, во-первых, сама инфраструктура такого банка достаточно редко управляется централизовано поэтому они не способны оперативно сменить пароли. Во-вторых, небольшой состав подразделения, занимающегося вопросами информационной безопасности, не позволяет быстро реагировать на атаки. В-третьих, низкий уровень подготовки персонала, а именно отсутствие профильных навыков по поиску несанкционированной активности, четких процедур по самостоятельному выявлению вредоносного программного обеспечения. В-четвертых, человеческий фактор, а именно халатность сотрудников, не исполняющих рекомендации по устранению последствий хакерских атак, приводящих впоследствии к повторным атакам. И именно кредитно-финансовые организации входят в число наиболее атакуемых[2].

Ущерб, полученный компанией от утечки или раскрытия ее информации, способен привести к потере конкурентных преимуществ, к санкциям со стороны регулирующих органов, упущенной коммерческой выгоде и т. д. Например, компания Victoria's Secrets была оштрафована на 50 тыс. долл. за то, что не обеспечила надлежащей защиты своего Web-сайта электронной коммерции, в результате чего пострадали 560 клиентов, персональные данные которых оказались скомпрометированными[3].

2 Посыпкина А., Чернышова Е. Почему банки оказались не готовы к атакам хакеров // РБК.Ру, 19.02.2019. [WWW документ]. URL https://www.rbc.ru/technology_and_media/19/02/2019/5c6ac5439a794715806d3d6b (дата обращения 29.08.2019).

3 Главные утечки информации 2018 года // ItWeek, 27.12.2018. [WWW документ]. URL https://www.itweek.ru/security/news-company/detail.

Размер ущерба, которые понесли российские компании за 2017–2018 гг. составил:

2017 г. Почти каждая пятая компания понесла убытки от кибератак. Примерно 600 млрд руб. Убытки составили порядка 1 трлн руб.

Крупный бизнес — 62 %, малый и средний бизнес — 46–47 %.

Средняя сумма убытков в одной российской компании в 2017 г. составила около 300 тыс. руб., в крупном бизнесе — почти 900 тыс. руб., в финансово-кредитном секторе потери только одной организации составили свыше 500 тыс. руб.

Основными причинами стали: заражение вирусом компьютеров сотрудников компании с последующим вымогательством денег — 20 %, взлом почтовых ящиков — 12%, атаки на сайт компании — 10 %[4,5].

2018 г. Потери в целом составили около 1,1 трлн руб. Однако стоит отметить, что в 2018 г. потери финансово-кредитных организаций от кибератак снизились: за восемь месяцев в 2018 г. банки потеряли всего 76,5 млн руб[6].

В процессе своего развития компания/фирма неизбежно сталкивается с тем, что необходимо выработать целый ряд мероприятий, связанных с управлением ее информационной безопасностью. Для надежной и эффективной работы компании по предупреждению инцидентов существует необходимость в создании отлаженной структуры по обеспечению информационной безопасности, в организации специального отдела. Результаты исследования компании «Код безопасности» показали, что чем крупнее компания, тем выше осознание необходимости в создании специального ИБ-отдела. Так, в 71 % крупных российских компаний за обеспечение процессов информационной безопасности отвечает специализированный ИБ-отдел или ИБ-специалист. У компаний среднего размера данный показатель составляет 49 %, а в малых компаниях лишь 44 %. К сожалению, сегодня, большинство компаний и организаций возлагают ответственность за обеспечение информационной безопасности на ИТ-подразделения или другие отделы, либо предпочитают прибегать к помощи аутсорсинговых ИБ-специалистов. В 2019 г. наметилась тенденция сокращения количества российских компаний, в которых за обеспечение процессов информационной безопасности отвечает профильный отдел или специалист[7] [Парфенов, Стахно, 2016].

Наличие стратегии информационной безопасности компании повышает эффективность защиты ее информации. Поэтому правильно выстроенная стратегия будет способствовать как распределению финансовых и человеческих ресурсов в этом направлении, так и внедрению организационных и технических мер по обеспечению информационной безопасности в компании.

В настоящее время к основным мерам, которые принимают компании для защиты своей информационной безопасности, относятся[8] [Никонов, Павлов, 2016]:

1. Установка антивируса.
2. Проведение политики информационной безопасности в компании.
3. Ограничение доступа сотрудников в Интернет.
4. Обучение информационной безопасности.
5. Требования обязательной аттестации.
6. Доля компаний, которые используют указанные выше меры, показан на рисунке 2.

Сюда следует также отнести и заложенные в бюджет компании средства на информационную безопасность. Однако именно эта мера пока еще полностью не оценена руководством компаний. В большинстве компаний малого и среднего бизнеса выделяется достаточно скромный бюджет, рассчитанный только на стандартные меры, которых явно недостаточно для защиты от серьезных угроз.

php?ID=204871 (дата обращения 29.08.2019).

4 Девяткина М. Россия потеряла из-за кибератак 600 млрд руб. за 2017 г. // РБК.Ру, 16.10.2018. [WWW документ]. URL https://www.rbc.ru/society/16/10/2018/5bc5d6f49a7947f779d76eaf (дата обращения 29.08.2019).

5 Ли И. Российские компании за год потеряли более 100 млрд руб. из-за кибератак // РБК.Ру, 19.12.2017. [WWW документ]. URL. https://www.rbc.ru/technology_and_media/19/12/2017/5a38f3749a794710aa15581b (дата обращения 29.08.2019).

6 Компромисс бюджета и безопасности // Positive Technologies, 26.12.2018. [WWW документ]. URL. https://www.ptsecurity.com/ru-ru/research/analytics/regional-information-security-2018/ (дата обращения 29.08.2019).

7 Информационная безопасность на практике. Итоги 2018 г., перспективы 2019 г. Аналитическое исследование / ООО «Код Безопасности». [Электронный ресурс]: текст. URL https://www.securitycode.ru/upload/iblock/119/Info_Security_in_practice_2019.pdf

8 Ли И. Российские компании за год потеряли более 100 млрд руб. из-за кибератак // РБК.Ру, 19.12.2017. [WWW документ]. URL https://www.rbc.ru/technology_and_media/19/12/2017/5a38f3749a794710aa15581b (дата обращения 29.08.2019).

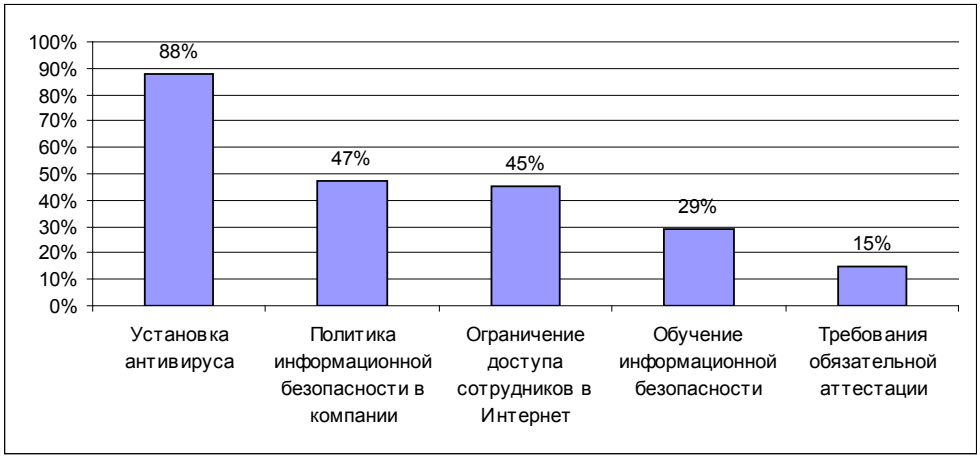

Рис. 2. Меры, принимаемые компаниями для защиты информации

Источник: рисунок автора по данным: Ли И. Российские компании за год потеряли более 100 млрд руб. из-за кибератак // РБК.Ру, 19.12.2017. [WWW документ]. URL https://www.rbc.ru/technology_and_media/19/12/2017/5a38f3749a794710aa15581b (дата обращения 29.08.2019).

Необходимость формирования бюджета компании на информационную безопасность во многом зависит от размеров информационной инфраструктуры компании, от оценки возможных рисков, от особенностей бизнес-процессов фирмы [Домбровская, Яковлева, Стахно, 2016]. Так, результаты проведенного аналитического исследования за 2019 г. показали, что доля бюджета, выделяемого на информационную безопасность составляет:

- государственный сектор — 18 %,
- финансовый сектор —17 %,
- промышленный сектор —15%,
- образование — 4 %[1].

Согласно исследованиям Anti-Malware.ru, 63 % российских компаний тратят на информационную безопасность не больше 500 тыс. руб. в год. Только 12 % организаций и предприятий выделяют бюджет больше 10 млн руб. и 6 % — больше 50 млн руб. При этом всего в 48 % компаний есть определенные планы развития, связанные с информационной безопасностью, и стратегия действий на будущее. В остальных 52 % компаний выделяемых денег, согласно заключениям аналитиков Рамблер, хватает лишь на текущие задачи без постановки средне- и долгосрочных целей[2].

В соответствии с Альманахом кибербезопасности Cisco/Cybersecurity 2019 «…коммерческие организации по всему миру, согласно отчету Gartner, потратили порядка 87 миллиардов долларов на нужды кибербезопасности в 2017 г., включая софт, специализированные сервисы и «железо». Это на 7 % больше, чем в 2016 г. В 2018 г. цифра 93 миллиардов, в 2019 г. перевалит отметку в 100 миллиардов. По оценкам экспертов, в России объем рынка услуг информационной безопасности составляет порядка 55–60 миллиардов руб. (около 900 тыс. долларов). На 2/3 его закрывают государственные заказы. В корпоративном секторе доля таких затрат сильно зависит от формы компании/предприятия, географии и сферы деятельности. Отечественные банки и финансовые структуры в среднем вкладывают в свою кибербезопасность 300 млн руб. в год, промышленные предприятия и компании (малый и средний бизнес) — до 50 млн руб., сетевые компании (ритейл) — от 10 до 50 млн руб.»[3].

Согласно специальному отчету Cisco по кибербезопасности, «…злоумышленники рассматривают малый и средний бизнес как слабые цели с менее сложной инфраструктурой и практикой обеспечения безопасности, а также с недостаточным количеством обученного персонала для управления угрозами и реагирования на них. Почти половина всех кибератак совершается против малого бизнеса. Для этих компаний главными проблемами безопасности являются целевые фишинговые атаки на сотрудников, постоянные угрозы, вымогательство, атаки типа «отказ в обслуживании» и рост числа сотрудников, которым разрешено

1 Информационная безопасность на практике. Итоги 2018 г., перспективы 2019 г. Аналитическое исследование / ООО «Код Безопасности». [Электронный ресурс]: текст. URL https://www.securitycode.ru/upload/iblock/119/Info_Security_in_practice_2019.pdf

2 Информационная безопасность: сколько за нее платят в России? // Kickidler. [WWW документ]. Платный доступ: https://www.kickidler.com/ru/info/informacziionnaya-bezopasnost-skolko-za-nee-platyat-v-rossii.htm, (дата обращения 29.08.2019).

3 Morgan S. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics // Cybersecurity Ventures, 06.02.2019. [WWW документ]. URL https://cybersecurityventures.com/cybersecurity-almanac-2019/ (дата обращения 29.08.2019).

использовать собственные мобильные устройства»[4].

По мнению экспертов по безопасности Cisco «…предприятия малого/среднего бизнеса более склонны выплачивать выкуп злоумышленникам, для того, чтобы они могли быстро возобновить нормальную работу после атаки вымогателей. Компании просто не могут позволить себе простои и отсутствие доступа к критически важным данным, включая данные клиентов»[5].

Следует отметить, что из опрошенных руководителей компаний малого и среднего бизнеса, знающих о существовании информационных угроз, 60 % руководителей считает риск минимальным. Это и является основной проблемой, связанной с сохранением и защитой информации в компании, а именно — недооценка последствий[6].

К основным сдерживающим факторам, которые препятствует выделению средств на обеспечение информационной безопасности компании, следует отнести следующие.

- Недостаточный уровень информированности высшего руководства в вопросах информационной безопасности.
- Показатели безопасности являются слишком техническими, что затрудняет понимание значимости вопроса.
- Возможные потери в результате ИБ-рисков руководство считает меньшими по сравнению с затратами на развитие системы информационной безопасности.
- Ограниченный бюджет[7] [Хурум, 2018].

Сегодня в России пока еще мало структур, занимающихся вопросами и анализом информационной безопасностью компаний.

Самой известной на сегодняшний день является группа компаний InfoWatch, которая специализируется на информационной безопасности в корпоративном секторе: защите корпораций от утечек информации и целевых атак извне. Компания контролирует около 50 % российского рынка систем защиты. Также, вопросами, связанными с информационной безопасностью, активно занимается компания SearchInform (ООО «СёрчИнформ») — производитель программного обеспечения для защиты от утечек информации (DLP), контроля продуктивности сотрудников за ПК и управления событиями информационной безопасности (SIEM). Еще одной известной структурой, которая проводит исследования и анализ в области информационной безопасности, является аналитический центр НАФИ — специализирующийся на изучении общественного мнения (социология), предпринимательского климата (экономика), потребительского поведения (маркетинг), а также на анализе статистики, макроэкономических данных и открытой информации.

Также на российском рынке присутствует компания Positive Technologies, которая является одним из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений.

В связи с нарастающими каждый год угрозами утечки информации необходимо при сутствие на этом рынке как можно большего числа компаний, которые могли бы не только проводить анализ проблем, но и консультировать, предоставлять необходимое оборудование, проводить обеспечение для защиты информации фирмы или организации.

Ни одна сфера управления и ведения бизнеса не обходится без информационных технологий. Возможности поиска и обмена информацией в Интернете стремительно развиваются. Необходимо четко понимать, что слабая информационная безопасность способна привести не только к финансовым, имиджевым и прочим потерям, но и поставить под угрозу все существование бизнеса. Поэтому необходимо учитывать при разработке стратегии фирмы вопросы и проблемы, связанные с информационной безопасностью и уделять им повышенное внимание.

Данное обстоятельство также необходимо учитывать в рамках теории фирмы, поскольку в настоящее время информационная безопасность зачастую играет даже большую роль, чем безопасность физическая. Исследование информационных границ фирмы и возможных утечек информации показывает, что для обеспечения безопасности в данной сфере необходимо использовать междисциплинарный подход. Помимо организации безопасного сетевого взаимодействия внутри фирмы и за ее пределами, традиционно ис-

4 Там же.

5 Там же.

6 Ли И. Российские компании за год потеряли более 100 млрд руб. из-за кибератак // РБК.Ру, 19.12.2017. [WWW документ]. URL https://www.rbc.ru/technology_and_media/19/12/2017/5a38f3749a794710aa15581b (дата обращения 29.08.2019).

7 Информационная безопасность на практике. Итоги 2018 г., перспективы 2019 г. Аналитическое исследование / ООО «Код Безопасности». [Электронный ресурс]: текст. URL https://www.securitycode.ru/upload/iblock/119/Info_Security_in_practice_2019.pdf

следуемых в рамках информатики, здесь также должны использоваться результаты таких дисциплин как психология, социология, история, экономика и юриспруденция и др.

Список источников

Балановская А. В. Источники возникновения и последствия реализации угроз информационной безопасности промышленных предприятий // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент», №13, 2015. С. 63–75.

Васильев И. И., Портнов М. С. Правовые основы защиты конфиденциальной информации в коммерческих организациях // Вестник российского университета кооперации. №3 (21), 2015. С. 95–98.

Волокитин А. В. и др. Информационная безопасность государственных организаций и коммерческих фирм / А. В. Волокитин, А. П. Маношкин, А. В. Солдатенков, С. А. Савченко, Ю. А. Петров М.: ФИОРД-ИНФО, 2002. 272 с.

Годырева А. В. Возможные каналы утечки информации на предприятии // Научно-технический вестник информационных технологий, механики и оптики. № 6 (51), 2008. С. 146–151.

Домбровская Л. А., Яковлева Н. А., Стахно Р. Е. Современные подходы к защите информации, методы, средства и инструменты защиты // Наука, техника и образование, № 4 (22). 2016. С. 16–19.

Дорофеев А. В., Марков А. С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. №1 (2), 2014. С. 67–73.

Клейнер Г. Б., Рыбачук М. А. Междисциплинарная теория фирмы: ключевые положения, отличительные черты // Стратегическое планирование и развитие предприятий. Секция 1 / Материалы Двадцатого всероссийского симпозиума. Москва, 9–10 апреля 2019 г. Под ред. чл.-корр. РАН Г. Б. Клейнера. Москва: ЦЭМИ РАН, 2019. С. 60–64.

Максимов Ю. Н., Сонников В. Г. и др. Шпионские штучки. Технические методы и средства защиты информации. СПб: Полигон, 2000. 320 с.

Никонов А. И., Павлов Н. О. Системы защиты информации и их место в политике безопасности // Вестник НГИЭИ, № 8 (63), 2016. С. 48–54.

Парфенов Н. П., Стахно Р. Е. Технология защиты персональных данных // Наука, техника и образование, № 4 (22), 2016. С. 15–16.

Рыбачук М. А. Междисциплинарная теория фирмы: структуризация внутреннего наполнения и внешнего окружения предприятия // Междисциплинарность в современном социально-гуманитарном знании — 2018: материалы Третьей международной научной конференции (Ростов-на-Дону, 20–22 сентября 2018 г.). Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2018. Т. 2. Секционные доклады. Ч. 1. С. 143–152.

Хурум М. А. Социальная обусловленность криминализации деяний, связанных с получением и разглашением конфиденциальной информации, составляющей коммерческую тайну // Гуманитарные, социально-экономические и общественные науки, № 4. 2018 С. 172–176.

RUSSIAN MANAGEMENT: A MODERN PERSPECTIVE

Ekaterina Akinfeeva[1]

INFORMATION SECURITY AS A FACTOR OF EFFECTIVE ACTIVITY OF THE COMPANY

Abstract. The relevance of the study is due to the fact that weak information security can lead not only to economic, financial and other losses, but also threaten the entire existence of the business. Therefore, it is necessary to take into account the issues and problems related to information security in the development of the strategy of the company/firm and pay special attention to them. In this regard, this article aims to analyze the main issues and problems associated with the leakage of company information.

The article provides a brief analysis of the situation related to the information security of the company, its protection and preservation. The General statistical data on information leakage, on the main Russian structures, the companies and the organizations which are most exposed to information leakage are presented. The amount of damage received by Russian companies in 2017–2018 and the measures taken by companies to protect themselves are shown.

The materials of the article are of practical value for firms/companies to prevent incidents related to existing threats of information leakage.

Key words: information, confidential information, cyberattack, hackers, company data leakage, amount of damage, data protection, company strategy.

JEL: M15

1 **Akinfeeva Ekaterina Vladimirovna** – Candidate of Sci. (Econ.), associate Professor. Central economic and mathematical Institute of RAS (CEMI RAS). Moscow, Russia. E-mail: katerina@cemi.rssi.ru. **AuthorID: 428058**

References

Balanovskaya A. V. Istochniki vozniknoveniya i posledstviya realizatsii ugroz informatsionnoy bezopasnosti promyshlennykh predpriyatiy [Sources of occurrence and consequences of the implementation of threats to the information security of industrial enterprises]. *Nauchnyy zhurnal NIU ITMO. Seriya "Ekonomika i ekologicheskiy menedzhment" = Scientific journal NRU ITMOSeries "Economics and Environmental Management",* No. 13, 2015. P. 63–75.

Vasil'yev I. I., Portnov M. S. Pravovyye osnovy zashchity konfidentsial'noy informatsii v kommercheskikh organizatsiyakh [Legal basis for the protection of confidential information in commercial organizations]. *Vestnik rossiyskogo universiteta kooperatsii = Vestnik of the Russian University of Cooperation*. No. 3 (21), 2015. P. 95–98.

Volokitin A. V. et al. *Informatsionnaya bezopasnost' gosudarstvennykh organizatsiy i kommercheskikh firm* [Information Security of State Organizations and Commercial Firms] / A. V. Volokitin, A. P. Manoshkin, A. V. Soldatenkov, S. A. Savchenko, Yu. A. Petrov. Moscow: FIORD-INFO Publ., 2002. 272 p.

Godyreva A. V. Vozmozhnyye kanaly utechki informatsii na predpriyatii [Possible channels of information leakage at the enterprise]. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki = Scientific and Technical Journal of Information Technologies, Mechanics and Optics.* No. 6 (51), 2008. P. 146–151.

Dombrovskaya L. A., Yakovleva N. A., Stakhno R. E. Sovremennyye podkhody k zashchite informatsii, metody, sredstva i instrumenty zashchity [Modern approaches to information protection, methods, means and tools of protection]. *Nauka, tekhnika i obrazovaniye = Science, Technology and Education*, No. 4 (22). 2016. P. 16–19.

Dorofeyev A. V., Markov A. S. Menedzhment informatsionnoy bezopasnosti: osnovnyye kontseptsii [Information Security Management: Basic Concepts]. *Voprosy kiberbezopasnosti* [Cybersecurity Issues]. No. 1 (2), 2014. P. 67–73.

Kleyner G. B., Rybachuk M. A. Mezhdistsiplinarnaya teoriya firmy: klyuchevyye polozheniya, otlichitel'nyye cherty [Interdisciplinary theory of the company: key points, distinguishing features]. *Strategicheskoye planirovaniye i razvitiye predpriyatiy. Sektsiya 1. Materialy Dvadtsatogo vserossiyskogo simpoziuma* [Strategic planning and development of enterprises. Section 1. Proceedings of the Twentieth All-Russian Symposium]. Moscow, April 9–10, 2019, Ed. G. B. Kleiner. Moscow: CEMI RAS Publ., 2019. P. 60–64.

Maksimov Yu. N., Sonnikov V. G. et al. *Shpionskiye shtuchki. Tekhnicheskiye metody i sredstva zashchity informatsii* [Spy things. Technical methods and means of information protection]. St. Petersburg: Polygon Publ., 2000. 320 p.

Nikonov A. I., Pavlov N. O. Sistemy zashchity informatsii i ikh mesto v politike bezopasnosti [Information security systems and their place in the security policy]. *Vestnik NGIEI = Bulletin NGIEI*, No. 8 (63), 2016. P. 48–54.

Parfenov N. P., Stakhno R. E. Tekhnologiya zashchity personal'nykh dannykh [Technology for the protection of personal data]. *Nauka, tekhnika i obrazovaniye = Science, Technology and Education*, No. 4 (22), 2016. P. 15–16.

Rybachuk M. A. Mezhdistsiplinarnaya teoriya firmy: strukturizatsiya vnutrennego napolneniya i vneshnego okruzheniya predpriyatiya [Interdisciplinary theory of the company: structuring the internal content and external

environment of the enterprise]. *Mezhdistsiplinarnost' v sovremennom sotsial'no-gumanitarnom znanii – 2018: materialy Tret'yey mezhdunarodnoy nauchnoy konferentsii (Rostov-na-Donu, 20–22 sentyabrya 2018 g.)* [Interdisciplinarity in modern social and humanitarian knowledge – 2018: Proceedings of the Third International Scientific Conference (Rostov-on-Don, September 20–22, 2018). Rostov-on-Don; Taganrog: Southern Federal University Publ., 2018. Vol. 2. Section reports. Part 1. P. 143–152.

Khurum M. A. Sotsial'naya obuslovlennost' kriminalizatsii deyaniy, svyazannykh s polucheniyem i razglasheniyem konfidentsial'noy informatsii, sostavlyayushchey kommercheskuyu taynu [Social conditionality of criminalization of acts related to the receipt and disclosure of confidential information constituting a trade secret]. *Gumanitarnyye, sotsial'no-ekonomicheskiye i obshchestvennyye nauki* [Humanitarian, Social, Economic and Social Sciences], No. 4. 2018 P. 172–176.