Таким образом, внедрение цифровых технологий, на современном этапе информационного развития, является главным звеном в системе экономической безопасности предприятия.

ЛИТЕРАТУРА

1. Глазьев С.Ю. Великая цифровая революция. URL: http://www.glazev.ru/articles/6-jekonomika/54923-velikaja-ts ifrovaja-revoljutsi ja-vyzovy-i-perspektivy-dl ja-jekonomiki-i-veka.

2. Глазьев С.Ю. Экономика будущего. Есть ли у России шанс? М.: Книжный мир, 2017.

3. Лавриненко Е.А., Чмирева Е.В. ИНСТРУМЕНТАЛЬНОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ УПРЕЖДАЮЩЕГО МОНИТОРИНГА ИНВЕСТИЦИОННЫХ ПРОЕКТОВ // Фундаментальные исследования. – 2018. – № 4. – С. 104-108; URL: http://fundamental-research.ru/ru/article/view?id=42126 (дата обращения: 14.05.2019).

3. Федеральная служба государственной статистики. URL: www.gks.ru (дата обращения: 25.01.2018).

4. Комплексная оценка уровня экономической безопасности Белгородского региона / Бондарева Я.Ю., Герасимова Н.А., Дружникова Е.П., Кулик А.М., Стрябкова Е.А. В книге: Факторы устойчивого развития регионов России Бондарева Я.Ю., Верещагина Л.В., Ворожейкина Т.М., Герасимова Н.А., Гришкова Д.Ю., Губа М.Н., Дружникова Е.П., Коокуева В.В., Кулик А.М., Покровская О.Д., Стрябкова Е.А. Монография. Под общей редакцией С.С. Чернова. Новосибирск, 2017. – С. 65-94.

О НЕКОТОРЫХ АСПЕКТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Г.А. Поддубный., В.А. Калугин
г. Белгород, Россия
Белгородский государственный национальный исследовательский университет

В статье рассмотрены основные аспекты, связанные с определением и регулированием информационной безопасности в РФ, приведены некоторые из возможных угроз информационной безопасности РФ, а также статистика совершенных кибератак на основные отрасли РФ.

Ключевые слова: *информация, информационная безопасность, информационная угроза, сертификация, информационное воздействие, компьютерная атака.*

ON SOME ASPECTS OF INFORMATION SECURITY OF THE RUSSIAN FEDERATION

G. A. Poddubny., V. A. Kalugin
Belgorod, Russia
Belgorod state national research University

The article discusses the main aspects related to the definition and regulation of information security in the Russian Federation, presents some of the possible threats to information security of the Russian Federation, as well as statistics of cyber-attacks on the main sectors of the Russian Federation.

***Keywords**: information, information security, information threat, certification, information impact, computer attack.*

Информация всегда имела особое значение в общественной жизни, ценность информации зависит от того, какими преимуществами она наделяет обладающего ею. Организации собирают информацию о своих конкурентах и текущем состоянии рынка, тем самым получая конкурентные преимущества; страны собирают информацию для того, чтобы получить преимущества на мировой политической арене. В наше время объем информации возрастает экспоненциально, к тому же большая её часть оцифрована, что создает дополнительные возможности для лиц заинтересованных в её получении и использовании в корыстных целях. Все это повышает актуальность вопроса обеспечения информационной безопасности, как отдельных регионов, так и страны в целом.

Существует множество определений информационной безопасности, многие из которых основаны на определении из британского стандарта BS 7799 вышедшего в 1995 г., в котором сказано, что информационная безопасность – это защищенность ресурсов информационной системы от факторов, представляющих угрозу конфиденциальности, целостности и доступности[4]. В РФ основные цели, задачи, а также определение информационной безопасности прописаны в «Доктрине информационной безопасности Российской Федерации утвержденной УП РФ от 5 декабря 2016 г.».

В соответствии с данной доктриной информационная безопасность РФ – это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства[3]. Кроме этого в данном документе описаны основные угрозы информационной безопасности РФ, среди которых присутствуют:

- активизация экстремистских организаций использующих механизмы информационного воздействия на индивидуальное, групповое и общественное сознание с целью нагнетания межнациональной и социальной напряженности;
- увеличение масштабов компьютерной преступности, рост числа преступлений связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе касающейся неприкосновенности частной жизни при обработке персональных данных с использованием информационных технологий;
- увеличение сложности и скоординированности компьютерных атак на объекты критической информационной инфраструктуры[3].

Предотвращением данных угроз, а также иными вопросами информационной безопасности РФ занимаются две службы:

- ФСТЭК (Федеральная служба технического и экспортного контроля), в ее компетенцию входят вопросы сертификации средств защиты информации, противодействия иностранным техническим разведкам, аттестация рабочих мест по требованиям безопасности информации и т.д.
- ФСБ (Федеральная служба безопасности), а именно отдел лицензирования и сертификации, который обеспечивает защиту государственной тайны, отвечает за регулирование работы со средствами негласного получения информации, а также разработку и оборот технических средств криптографической защиты данных [3].

Из-за отсутствия единой службы, которая бы специализировалась только на вопросах информационной безопасности, возникают ситуации, когда комплексные технические средства и программные обеспечения попадают под регулирование сразу двух ведомств. Это приводит к лишней бюрократии, увеличению сроков сертификации и удорожанию конечного продукта, что в свою очередь влияет на своевременность вывода новейших средств информационной защиты.

Исходя из данных исследований Positive Technologies, за 2018 г. было проведено 1267 уникальных атак, основной целью которых являлось завладение конфиденциальной информацией[5]. На рисунке 1 приведены основные мотивы, которые преследовали лица совершившие данные атаки:

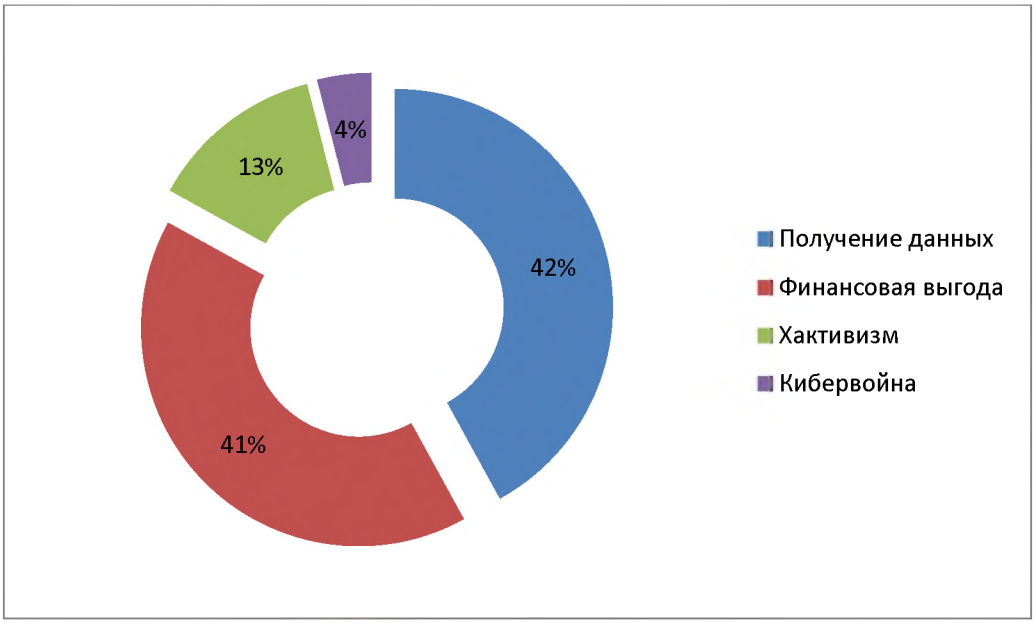

Рис. 1. Мотивы совершенных атак

Из данной диаграммы видно, что помимо завладения конфиденциальными данными, значительная доля кибератак была направлена на получение финансовой выгоды. Также следует отметить, что кража информации по большей степени несла финансовый подтекст, так как полученные данные подлежали дальнейшей продажи.

Подобным атакам в больше всего подвержены государственные учреждения, финансовая отрасль и медицинские учреждения. Более подробно приоритеты злоумышленников представлены на рисунке 2.

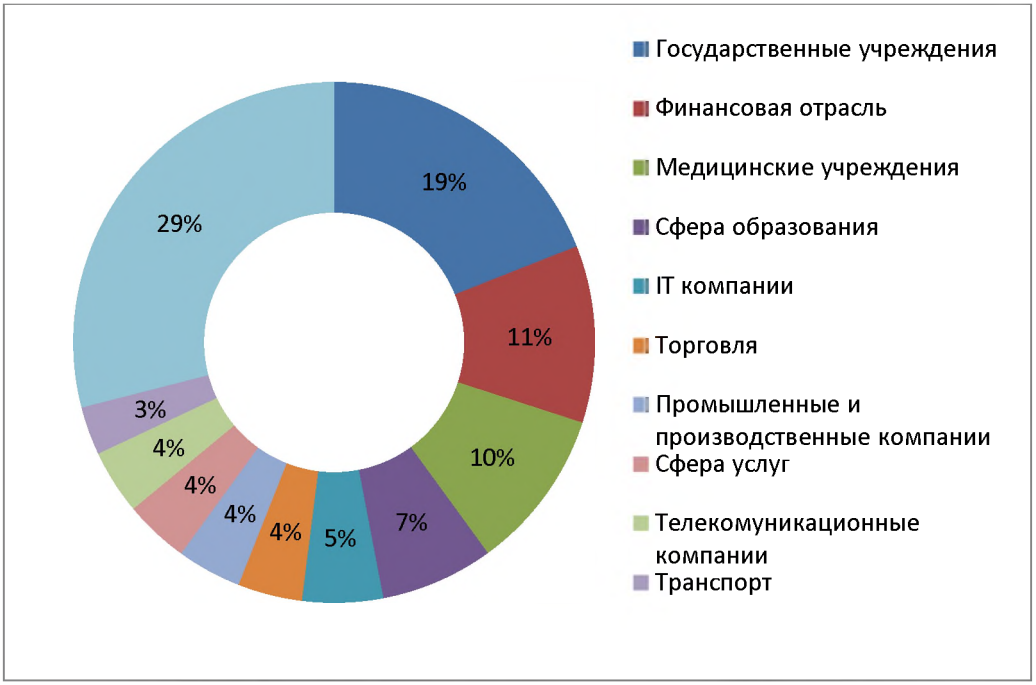

Рис. 2. Категории пострадавших от кибератак

Выбор основной целью государственные учреждения связан с недостатком финансирования обеспечения информационной безопасности, как правило, основным средством защиты от злоумышленников является антивирусная программа, и этого чаще всего недостаточно.

Что касается финансовой отрасли, то она всегда будет одной из основных целей подобных атак, так как является основным источником получения финансовых выгод злоумышленников. Согласно указанию № 4793-У Центрального банка РФ, с 1 января 2020 года ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры станут обязательными для всех операторов по переводу денежных средств и операторов услуг платежной инфраструктуры, что должно в значительной степени осложнить деятельность злоумышленников[3].

Защита всех составляющих требует разработки методического аппарата и создания собственной инфраструктуры. Задачи обеспечения информационной безопасности осложняются тем, что информационное пространство не имеет границ. Особенности работы сети Интернет и возможности беспроводной связи создают предпосылки для бесконтрольного и беспрепятственного переноса через рубежи государств огромных массивов данных, часто содержащих сведения, оборот которых в мире или в отдельных странах запрещен или ограничен. Атакующие технологии развиваются быстрее защитных, поэтому даже государственные базы данных находятся в зоне риска.

Исходя из вышесказанного можно сделать вывод, что угрозы информационной безопасности РФ определены верно, но из-за отсутствия единой службы отвечающей за защиту информации возникают проблемы своевременного вывода на рынок новейших решений позволяющих предотвращать потенциальные угрозы. Кроме того следует уделить особое внимание обеспечению информационной безопасности государственных учреждений.

ЛИТЕРАТУРА

1. Астахова Л.В. Теория информационной безопасности и методология защиты информации: учебное пособие – Челябинск: Издательский центр ЮУрГУ, 2014. – 137 с.

2. Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2014 – 372 с.: ил.

3. Родичев Ю.В. Нормативная база и стандарты в области информационной безопасности: учебник для вузов. – Питер, 2017. – 254 с

4. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2017. – 304 с.

5. Positive Technologies [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ (Дата обращения 17.03.2019).

6. Консультант плюс [Электронный ресурс]. Режим доступа: http://www.consultant.ru (Дата обращения 17.03.2019).