ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ТРАНСПОРТЕ: ВИДЫ, ПРИЧИНЫ И НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ

INFORMATION SECURITY INCIDENTS IN TRANSPORT: TYPES, CAUSES AND NEGATIVE CONSEQUENCES

L. Gruzdeva

Summary. Statistical analysis of relevant threats of information security in the world and Russia for 2018 is presented in article. Incidents of information security on water, air and railway transport are considered. As examples of incidents the attacks with use of the malicious software as most widespread method of cyber-attacks of malefactors are selected. The key principle of strategy of protection of transport information systems is formulated.

Keywords: transport information system, information security, information security incident, information threat, information attack.

Груздева Людмила Михайловна
К.т.н., доцент, Российский университет транспорта (РУТ-МИИТ), Москва
docentglm@gmail.com

Аннотация. В статье представлен статистический анализ актуальных угроз информационной безопасности в мире и России за 2018 г. Рассмотрены инциденты информационной безопасности на водном, воздушном и железнодорожном транспорте. В качестве примеров инцидентов выбраны атаки с использованием вредоносного программного обеспечения, как самого распространенного метода кибератак злоумышленников. Сформулирован ключевой принцип стратегии защиты транспортных информационных систем.

Ключевые слова: транспортная информационная система, информационная безопасность, инцидент информационной безопасности, угроза информационной безопасности, информационная атака.

Введение

В настоящее время является достоверным фактом то, что ни одна организация не зависимо ни от форм собственности, ни от отрасли экономики, ни от страны месторасположения, не застрахована от угроз информационной безопасности (кибератак). Данное обстоятельство вызвано тем, что мировая экономика становится все более зависима от цифровых технологий, а угрозы перманентно развиваются, становятся все более сложными и непредсказуемыми.

Транспортные информационные системы (ИС) так же не являются исключением, сети становятся все более открытыми и взаимосвязанными, что усугубляет проблему обеспечения безопасности информационных ресурсов и процессов [1]. Использование традиционных закрытых сетей не позволительно, так как не отвечает запросам современной цифровой экономики.

Несмотря на то, что по данным аналитического отчета компании Positive Technologies за 2018 г. только 1% информационных атак было совершено на объекты транспорта [2], нужно учитывать, что информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, функционирующие в сфере транспорта отнесены на законодательном уровне к критической информационной инфраструктуре [3]. Инциденты информационной безопасности [4] на транспорте могут привести к масштабным и губительным последствиям во многих отношениях — не только крупным финансовым затратам на восстановление инфраструктуры, но и к человеческим жертвам.

Анализ статистических данных. Аналитический центр InfoWatch в 2018 г. зарегистрировал в мире 2263 случая утечки конфиденциальной информации, что на 6,2% больше, чем в 2017 г. и на +182,5%, чем в 2011 г. В результате скомпрометировано 7,28 млрд. записей. При этом доля умышленных утечек записей данных от общего числа утечек из информационных систем сферы промышленности и транспорта в 2018 г. составила 60,7% (рис. 1).

Россия с 2013 г. занимает второе место по числу утечек данных из защищаемых информационных систем, уступая первенство только Соединенным Штатам Америки [5]. Нарушители информационной безопасности успешно реализовали в 2018 г. угрозы с целью похищения следующих типов данных:

- персональные данные (69,5%);
- платежная информация (16,9%);
- государственная тайна (5,4%);
- коммерческая тайна, ноу-хау (8,1%).

Каналами утечек данных являются мобильные устройства, съёмные носители, электронная почта и бумажные документы, но лидирующее место занимают информационно-телекоммуникационные сети (браузер, cloud). В 2018 г. сеть была использована в 72,2% случаев утечек, что на 3% больше, чем было зафиксировано в 2017 г.

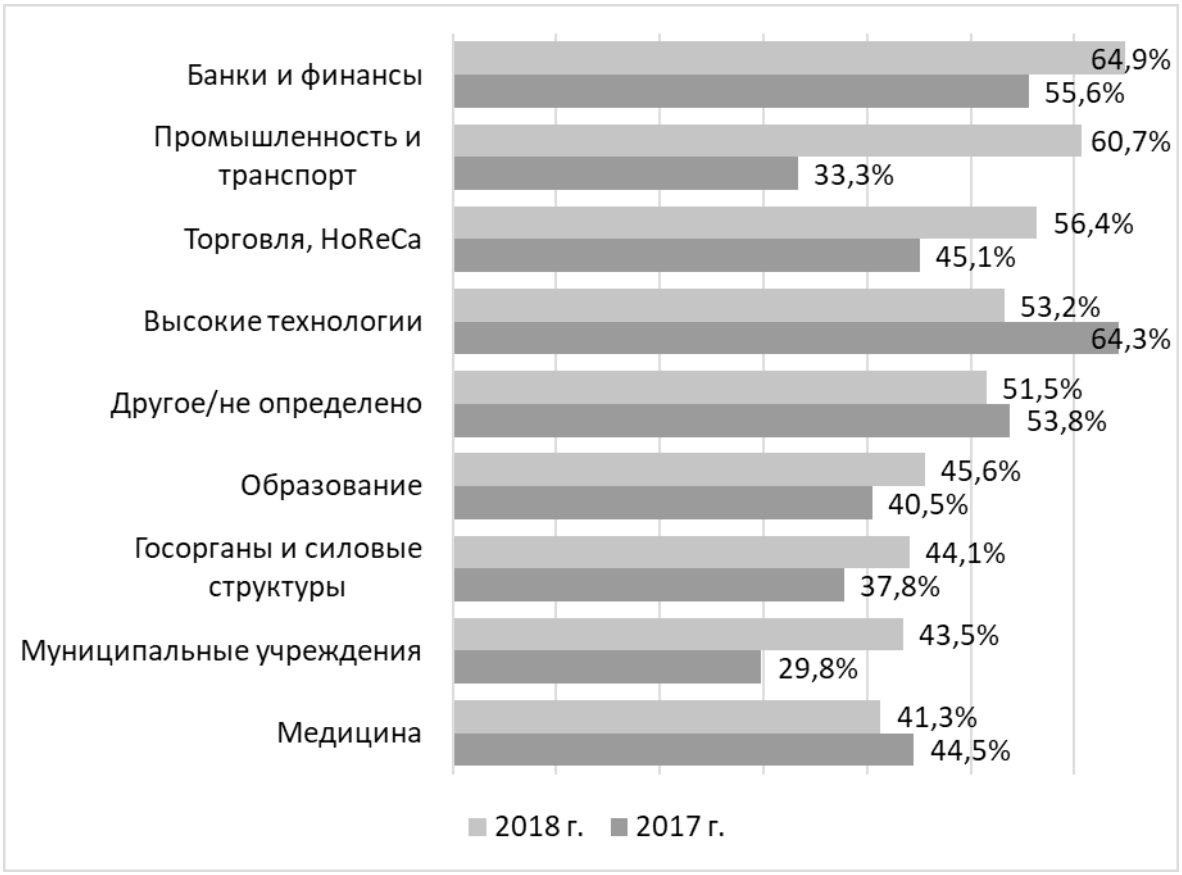

Рис. 1. Доля умышленных утечек записей данных от общего числа утечек по отраслям

Самым распространенным методом кибератак злоумышленников является использование вредоносного программного обеспечения (ПО), их доля в 2018 г. составила 56%. Данный метод нарушители информационной безопасности часто комбинировали с социальной инженерией и/или эксплуатацией веб-уязвимостей (рис. 2).

Примеры инцидентов информационной безопасности

Рассмотрим примеры атак с использованием вредоносного программного обеспечения на транспортные информационные системы.

В июне 2017 г. была совершена крупная кибератака с использованием вируса NotPetya на информационную инфраструктуру судоходного гиганта «Maersk Line» (Дания). Успешная реализация атаки привела к финансовым потерям компании, оцененные в 300 млн. долларов США. Данная сумма включает, среди прочего, потерю доходов и затраты на восстановление информационной системы.

Каналом реализации информационной угрозы послужила электронная почта. Сотрудник «Maersk Line» в Украине ответил на электронное письмо с вирусом NotPetya, результат его действий — повреждение ИС. Для решения данной проблемы и дальнейшего сдерживания угрозы, компания была вынуждена отключить заражённые сети, приостановив большинство операций. Это привело к почти полной остановке работы компании, так как был прекращён приём бронирований, контейнеровозы стояли в открытом море, а 76 портовых терминалов по всему миру остановили свою работу. Восстановление информационной инфраструктуры «Maersk Line» было осуществлено через восемь дней после атаки.

Реализация угрозы прошла успешно независимо от мер, которые «Maersk Line» предпринимает для предотвращения информационных инцидентов. В своем отчете за 2016 г. компания указала, что участвует в сложных и широкомасштабных глобальных проектах цифровизации своего бизнеса, что делает его в значительной степени зависимым от хорошо функционирующих ИС. Управление информационными рисками осуществляется посредством тщательного мониторинга, повышения устойчивости к кибератакам и особого внимания на непрерывное и надежное управление бизнесом даже при

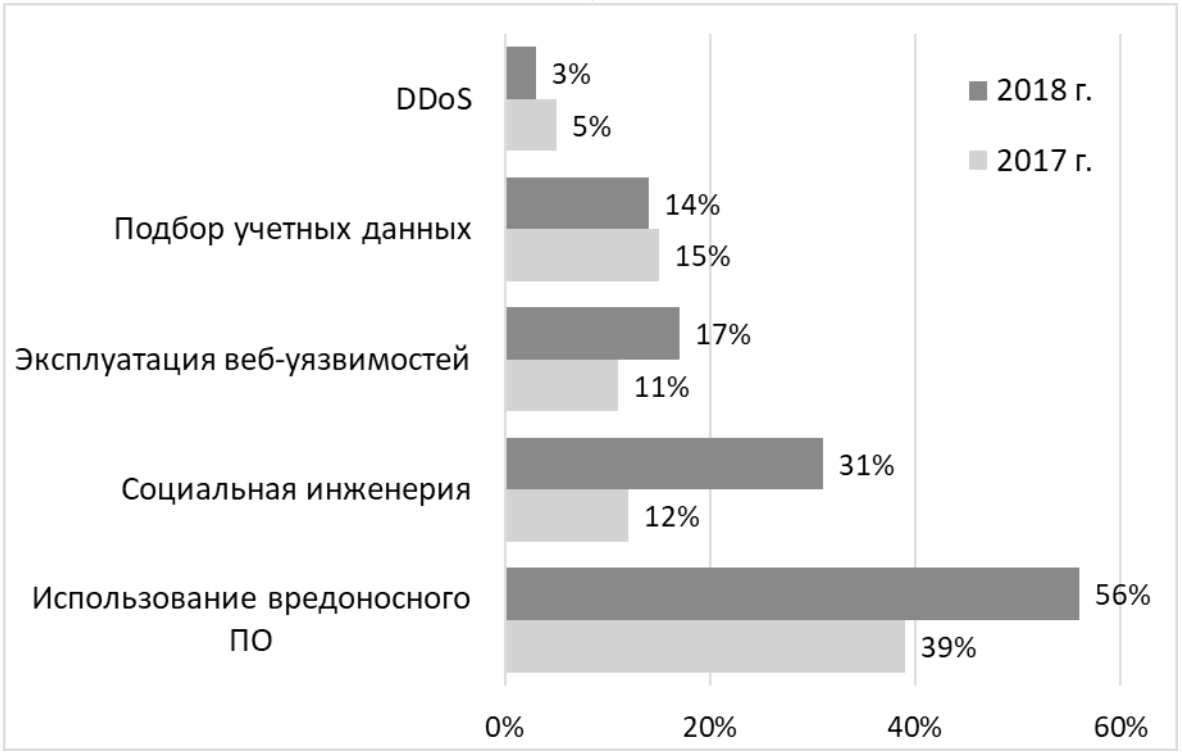

Рис. 2. Методы информационных атак

успешных атаках на информационные ресурсы компании.

После описанного инцидента для дальнейшего повышения устойчивости киберпространства в «Maersk Line» было реализовано и запланировано много немедленных и долгосрочных инициатив для защиты цифрового бизнеса, укрепления информационной инфраструктуры, повышения непрерывности и быстрого восстановления ИТ-услуг компании. Кроме того, компания застраховала риски от информационных инцидентов (киберстрахование) для смягчения некоторых потенциально возможных финансовых потерь от успешных кибератак в будущем.

Также с использованием вируса NotPetya в июне 2017 г. атаке был подвергнут украинский международный аэропорт Борисполь в Киеве. В результате инцидента, на некоторое время были отключены табло прилёта/вылета и сайт аэропорта. Работа аэронавигационных систем, также подвергнутых атаке, не была нарушена, самолёты прилетали и улетали по расписанию. Данное происшествие не нанесло серьёзного ущерба компании, однако, сказалось на её деятельности.

В сентябре 2018 г. атака с использованием программы-вымогателя NotPetya нарушила работу аэропорта Бристоля. Руководство аэропорта отказалось выполнять требования хакеров и выплачивать требуемую сумму для разблокировки информационных ресурсов. Как оказалось, целью злоумышленников являлся административный блок управления аэропортом, но достичь её не удалось, благодаря своевременно принятым мерам. Информационная система аэропорта вернулась к работе в штатном режиме через два дня.

По оценкам Европейского агентства по авиационной безопасности, около 1000 кибератак нацелены на авиационные системы во всем мире каждый месяц. В исследовании, проведенном Технологическим институтом Флориды (Florida Tech), перечисляются следующие элементы авиационной отрасли, которые потенциально уязвимы для кибератак: системы доступа, выезда и паспортного контроля, обработка грузов и доставка, системы управления полетом, управление полетным движением, перевозка опасных материалов, бортовой компьютер и навигационные системы, системы бронирования.

В мае 2017 г. компьютеры российских железных дорог были атакованы с помощью относительно нового семейства вымогателей WannaCry (WCry). Вирус заразил более 200 000 компьютеров в 150 странах в течение дня [6]. Специалисты по защите информации РЖД быстро локализовали инфекцию и железнодорожные перевозки не пострадали. Атаке с использованием WannaCry под-

верглась и информационная инфраструктура железнодорожной сети Германии Deutsche Bahn.

Эксперты считают, что вирус WannaCry использует уязвимость в программном обеспечении Microsoft Windows, впервые выявленную Агентством национальной безопасности США. После захвата компьютеров он отображал сообщения с требованием уплаты 300 долларов США (230 фунтов) в виртуальной валюте Биткойн, чтобы разблокировать файлы и вернуть их пользователю. Анализ BBC показал, что хакерам заплатили эквивалент £22,080 [7].

Заключение

Стратегии защиты транспортных информационных систем должны быть сформулированы с учетом одного ключевого принципа: ни одна защита не является неприступной. Независимо от мер по обеспечению информационной безопасности, которые предпринимают службы по защите информации, существует вероятность того, что информационные угрозы найдут «путь» для успешной реализации. Поэтому каждая организация должна быть готова реагировать и восстанавливаться путем создания кибер-устойчивости:

- быстро выявлять и реагировать на текущие нарушения информационной безопасности (кибератаки);
- устранять нарушение в системе безопасности и пытаться остановить потерю конфиденциальных данных и уменьшить потенциальный ущерб;
- применять извлеченные уроки из сложившейся ситуации для дальнейшего укрепления защиты и предотвращения повторных инцидентов информационной безопасности.

ЛИТЕРАТУРА

1. Securing the Transportation Network of Tomorrow [Электронный ресурс] // trendmicro.com: сайт.— URL: https://www.trendmicro.com/vinfo/ru/security/news/internet-of-things/securing-the-transportation-network-of-tomorrow.
2. Актуальные киберугрозы — 2018: тренды и прогнозы [Электронный ресурс] // Positive Technologies: сайт.— URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-rus.pdf.
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4. ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
5. Глобальное исследование утечек конфиденциальной информации в 2018 году [Электронный ресурс] // infowatch.ru: сайт.— URL: https://www.infowatch.ru/report2018.
6. Massive WannaCry/Wcry Ransomware Attack Hits Various Countries [Электронный ресурс] // blog.trendmicro.com: сайт.— URL: https://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-various-countries/.
7. Ransomware cyber-attack threat escalating — Europol [Электронный ресурс] // bbc.com: сайт.— URL: https://www.bbc.com/news/technology-39913630.

Журнал «Современная наука: актуальные проблемы теории и практики»