ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ТРАНСПОРТНОЙ ДЕЯТЕЛЬНОСТИ И ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

УДК 656(075.8):681

© Груздева Людмила Михайловна
— кандидат технических наук, доцент кафедры «Информационные технологии в юриспруденции» Юридического института Российского университета транспорта (МИИТ), профессор Российской Академии Естествознания (РАЕ)

Транспортная информационная инфраструктура как объект для компьютерных атак

Аннотация. Транспортные информационные системы в соответствии с действующим законодательством являются объектами критической информационной инфраструктуры Российской Федерации. В настоящее время обеспечению функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ уделяется повышенное внимание. В статье представлена статистика актуальных компьютерных атак, объектами которых являются различные отраслевые информационные инфраструктуры. Транспортные информационые ситемы России и мира были атакованы злоумышленниками с использованием вредоносного программного обеспечения в сочетании с социальной инженерией и эксплуатацией веб-уязвимостей. Одной из актуальных задач, стоящих перед специалистами служб защиты информации на транспорте, является предотвращение утечек информации по вине внутренних злоумышленников, использующих в том числе открытые каналы передачи данных.

Ключевые слова: информационная система; транспортная информационная инфраструктура; информационная безопасность; компьютерная атака; злоумышленник.

© Lyudmila M. Gruzdeva
— Candidate of Technical Sciences, associate professor of the department of informational technologies in jurisprudence, Law Institute of the Russian University of Transport, professor of the Russian Academy of Natural History (RANH)

Transport information infrastructure as an object for computer attacks

Abstract. In accordance with the current legislation, transport information systems are the objects of the critical information infrastructure of the Russian Federation. At present, there is paid an increased attention to ensuring the functioning of the state system of detection, prevention and elimination of the consequences of computer attacks on information resources of the Russian Federation. The paper presents the statistics of the current computer attacks, the objects of which are various sectoral information infrastructures. Transport information systems of Russia and of the world were attacked by cybercriminals using malicious software combined with social engineering and exploitation of web-based vulnerabilities. One of the urgent tasks facing the specialists of information protection services in transport is to prevent information leaks caused by internal intruders who use open data transmission channels.

Keywords: information system; transport information infrastructure; Information Security; computer attack; an intruder.

Компьютерная атака — целенаправленное воздействие программных и/или программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и/или прекращения их функционирования и/или создания угрозы безопасности обрабатываемой такими объектами информации. Данное определение было введено Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», после принятия которого гл. 28 Уголовного кодекса Российской Федерации была дополнена ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Согласно данной статье неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ, в том числе с использованием вредоносных компьютерных программ, влечет ответственность (в зависимости от целей злоумышленников, организации кибервоздействия, причиненного или возможного вреда) в виде лишения свободы на срок до 10 лет.

К субъектам критической информационной инфраструктуры отнесены государственные органы, государственные учреждения, российские юридические лица и индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы (ИС), информационно-

телекоммуникационные сети, автоматизированные системы управления, функционирующие в том числе в сфере транспорта.

По данным компании *Positive Technologies* — одного из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений, транспорт относится к категории жертв, пострадавших от атак в 2018 г. (рис. 1).

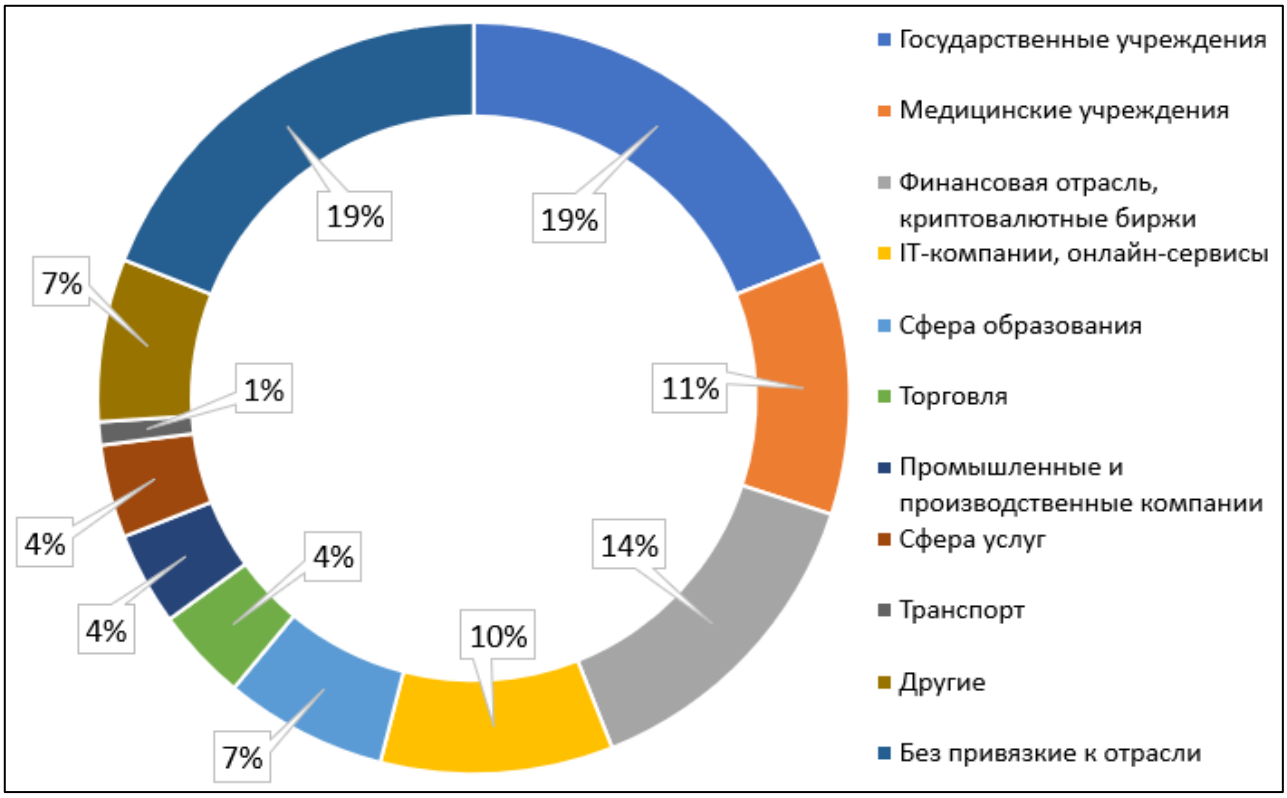

Рис. 1. **Категории жертв, пострадавших от атак 2018 г.**

Самым распространенным методом кибератак злоумышленников, в том числе для получения финансовой выгоды, являлось использование вредоносного программного обеспечения [1, 2], их доля в 2018 г. составила 56% (рис. 2). Например, в июне 2017 г. была совершена крупная кибератака с использованием вируса *NotPetya* на информационную инфраструктуру судоходной датской компании «*Maersk Line*». Успешная реализация атаки привела к финансовым потерям компании, оцененным в 300 млн долл. США. В мае 2017 г. информационная инфраструктура российских железных дорог (РЖД) была атакована с помощью вируса-вымогателя *WannaCry*. Вирус заразил более 200 тыс. компьютеров в 150 странах в течение дня [3]. Атака на ИС РЖД была локализована и перевозки не пострадали. Атаке с использованием *WannaCry* подверглась и информационная инфраструктура железнодорожной сети Германии *Deutsche Bahn*. А в сентябре 2018 г. атака с использованием программы-вымогателя *NotPetya* нарушила работу аэропорта Бристоля, ИС которого вернулась к работе в штатном режиме через два дня.

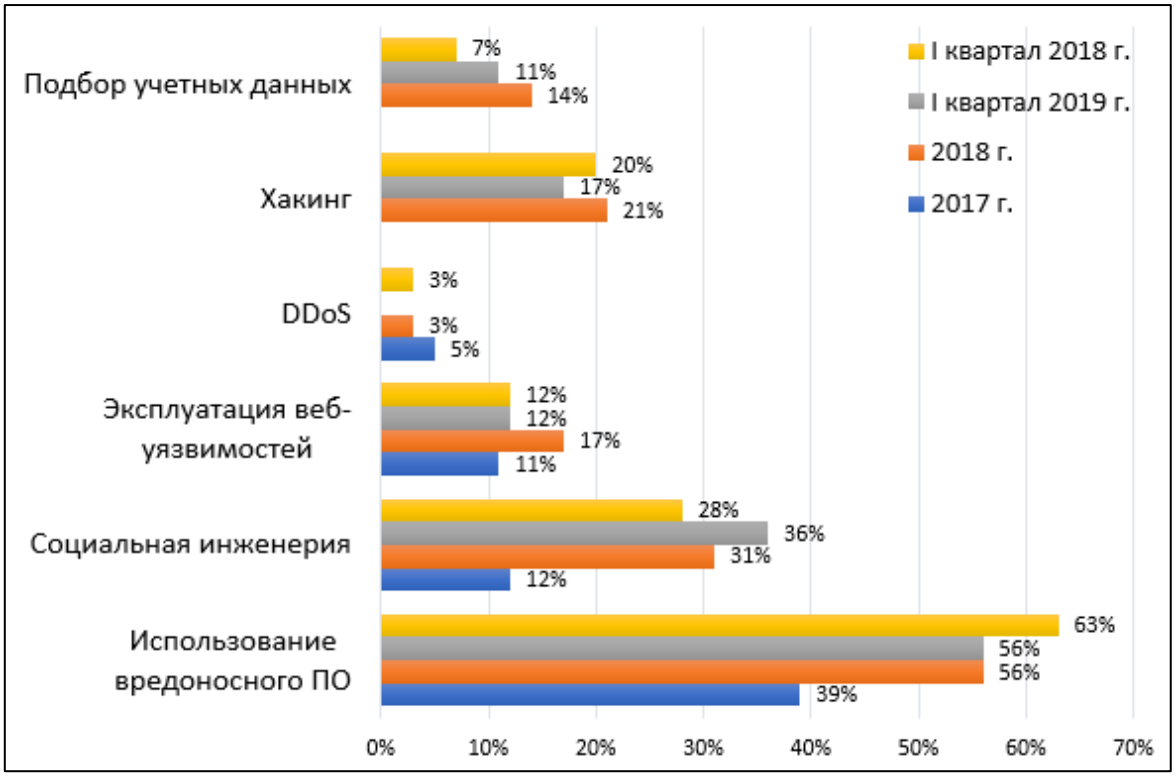

Рис. 2. **Методы атак**

Для формирования статистики об уязвимостях ИС за 2018 г. *Positive Technologies* выбрала 33 работы по анализу защищенности корпоративных информационных систем российских и зарубежных компаний из различных отраслей экономики, при этом доля транспортных ИС составила 15% [4].

Анализ защищенности проводился путем внешнего и внутреннего тестирования на проникновение в ИС [5]. На рис. 3 представлены наиболее распространенные уязвимости на сетевом периметре: словарные пароли пользователей, такие как *qwerty*, *admin*, 12345, 12345678, *guest* и т.д., использование открытых протоколов передачи данных. Злоумышленник может перехватить информацию, передаваемую по открытым протоколам без использования шифрования, и получить доступ к соответствующим ресурсам.

Рис. 3. **Наиболее распространенные уязвимости на сетевом периметре (доля системы)**

В середине марта 2018 г. программист Владимир Серов раскрыл самую крупную уязвимость в сервисе бесплатного *Wi-Fi* московского метро. Минимум год уязвимость позволяла злоумышленникам получать номера телефонов всех подключенных пассажиров поезда, а затем прочитать в незашифрованном виде цифровой портрет каждого: примерный возраст, пол, семейное положение, достаток, а также станции, на которых человек живет и работает [6].

The Village обнаружил, что по данным сервиса *Wayback Machine*, уязвимость была в коде страницы авторизации как минимум с 17 мая 2017 г. В августе компания заявляла, что идентификацию в сети ежедневно проходят 1,5 млн пользователей, а в декабре 2016 г. — что всего зарегистрировано более 12 млн пользователей. Эта же сеть *MT_FREE* сейчас доступна и в «Аэроэкспрессах», на Московском центральном кольце и даже в некоторых пригородных электричках, включая «Ласточки». А с 2017 г. «Максима» развивает ту же самую сеть в Петербургском метрополитене.

После публикации информации об уязвимости в сервисе *Wi-Fi* представитель кампании «МаксимаТелеком», предоставляющей доступ в интернет в Московском метрополитене, совместно с Департаментом транспорта г. Москвы и Московского метрополитена, сообщил о том, что передача профильных данных была оперативно зашифрована. В новом релизе системы авторизации в принципе не будет возможности загрузки

страниц с подменой MAC-адреса, что повысит устойчивость всей платформы к подобным атакам.

Помимо глобальных утечек существует еще множество способов взлома смартфонов через общедоступные точки доступа *Wi-Fi*. Самым распространенным является создание фальшивых сетей: злоумышленники создают сеть с похожим названием на общественную точку и дожидаются, когда к ней подключится невнимательный пользователь. Например, общественная точка доступа: «*MT_FREE*», а поддельная «*METRO_FREE*». После успешного подключения к точке доступа под различными предлогами выманиваются пароли от учетных записей или проводятся ряды атак. Наиболее частыми являются *MITM*-атаки различной сложности.

Смысл *MITM*-атаки (от англ. *Man-in-the-middle*) состоит в том, что хакер «прослушивает» весь трафик жертвы, в то время как она считает, что напрямую работает с нужными ей сайтами. Тем самым злоумышленник получает все логины и пароли, которые за это время ввел человек.

Так как социальная инженерия (метод несанкционированного доступа к информации или системам хранения информации без использования технических средств) — один из самых популярных и успешных способов проникновения в корпоративную ИС. компанией *Positive Technologies* были проведены проверки осведомленности сотрудников в вопросах информационной безопасности. Проверки осуществлялись путем телефонного взаимодействия и рассылки электронных писем. Почти треть пользователей перешла по ссылке или запустила приложенный файл, а каждый десятый сотрудник ввел свои учетные данные в фальшивую форму аутентификации (рис. 4).

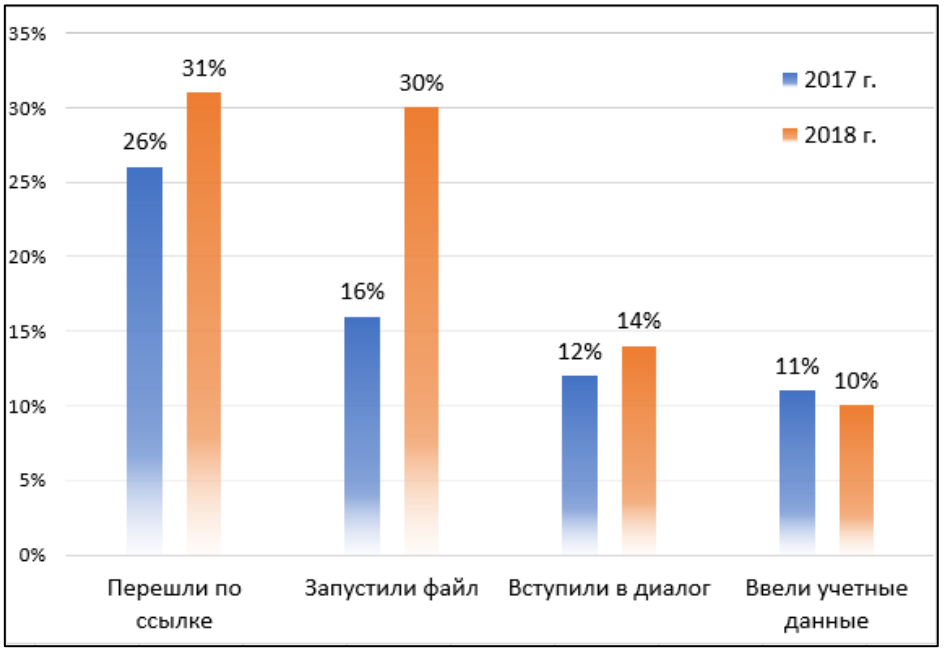

Рис. 4. **Результаты оценки осведомленности сотрудников**

Для предотвращения компьютерных атак, использующих социальную инженерию, необходимо регулярно проводить обучение сотрудников, направленное на повышение их компетенции в вопросах информационной безопасности, с контролем результатов.

По данным аналитического центра *InfoWatchB*, в географическом рейтинге Россия по числу информационных инцидентов, связанных с утечкой информации, в 2018 г. вновь заняла второе место, пропустив вперед только США [7]. При этом виновниками утечек информации являются сотрудники, руководители, а также системные администраторы, т. е. внутренние злоумышленники (рис. 5).

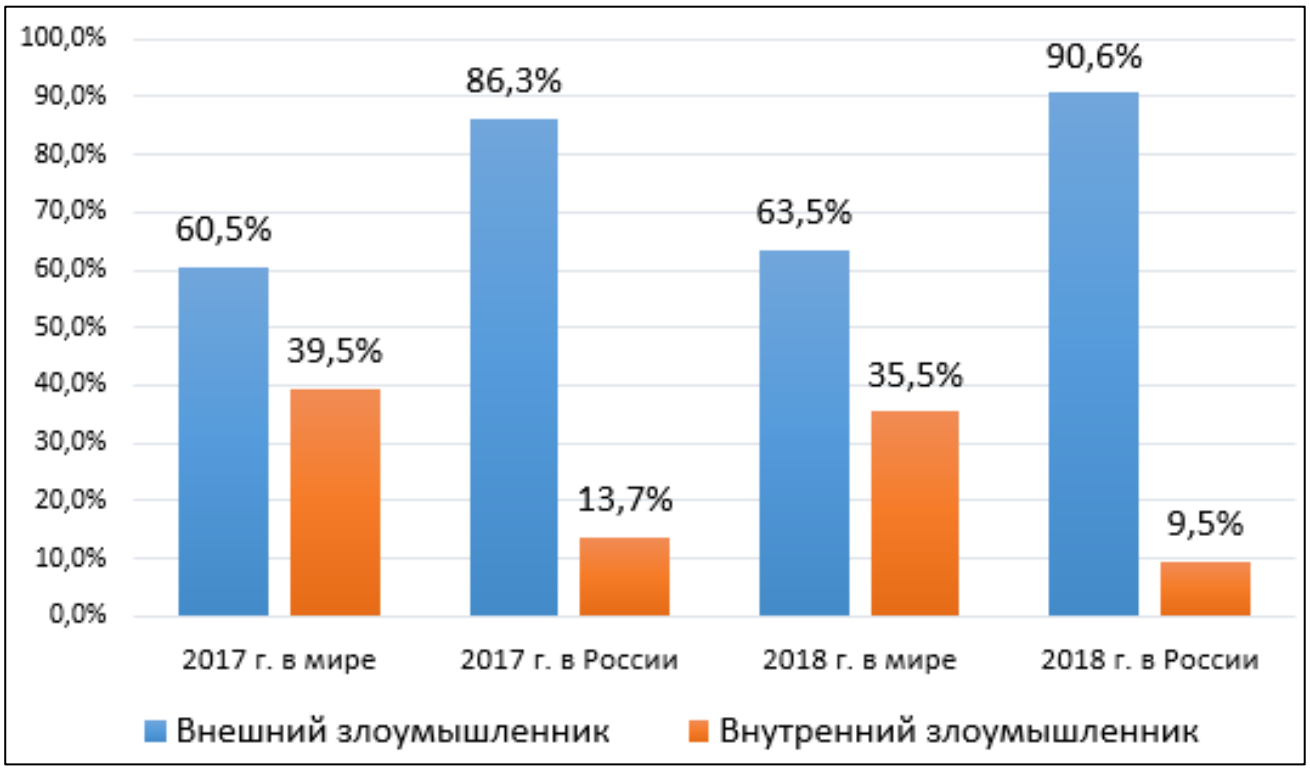

Рис. 5. **Распределение утечек по вектору воздействия, Россия — мир**

На рис. 6. приведена диаграмма, отражающая картину умышленных утечек конфиденциальной информации в различных отраслях экономики. В России доля умышленных утечек из транспортных информационных систем в 2018 г. возросла, что свидетельствую о «привлекательности» информации, циркулирующей в данных системах.

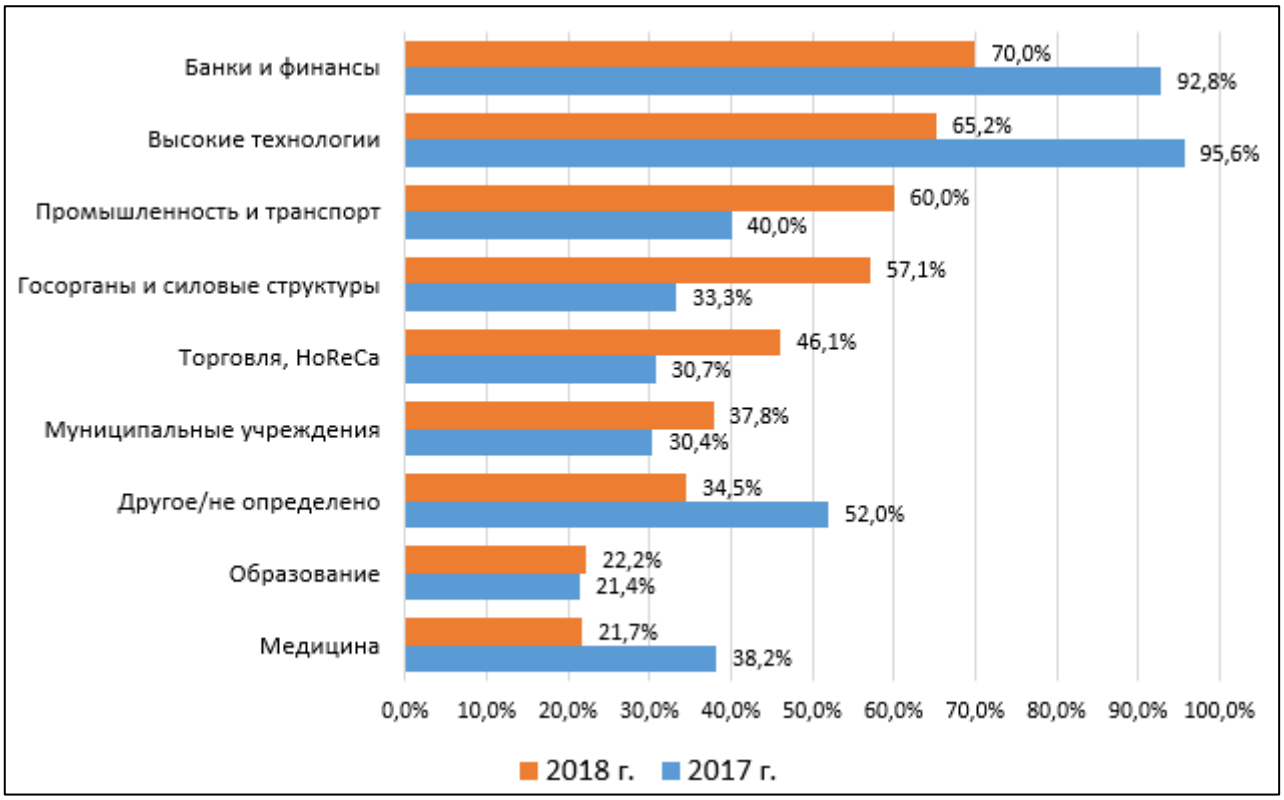

Рис. 6. **Доля умышленных утечек персональных данных и платежной информации по отраслям в Российской Федерации**

В связи со сложностью и актуальностью задачи обеспечения информационной безопасности критической информационной инфраструктуры с 1 января 2018 г. на ФСБ России возложены функции по обеспечению функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (см. Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»).

Задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ являются:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности информационных ресурсов Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

Литература

1. Актуальные киберугрозы — 2018: тренды и прогнозы // URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/.
2. Актуальные киберугрозы. I квартал 2019 года // URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/.
3. Massive WannaCry/Wcry Ransomware Attack Hits Various Countries // URL: https://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-various-countries/.
4. Уязвимости корпоративных информационных систем, 2019 // URL: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/.
5. Груздева, Л. М. Model of adaptive information security system of a computer-based data transmission network // Cloud of Science. — 2018. — Т. 3. — № 1.
6. Крупная утечка: Оператор Wi-Fi в метро Москвы выкладывает данные о пользователях в общий доступ // URL:https://www.the-village.ru/village/city/situation/308363-krupnaya-utechka-operator-wi-fi-v-metro-moskvy-vykladyvaet-dannye-o-polzovatelyah-v-obschiy-dostup/.
7. Глобальное исследование утечек конфиденциальной информации в 2018 году // URL: https://www.infowatch.ru/report2018.

References

1. Aktual'nyye kiberugrozy — 2018: trendy i prognozy [Actual cyber threats - 2018: trends and forecasts]// URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/.
2. Aktual'nyye kiberugrozy. I kvartal 2019 goda [Current cyber threats. I quarter of 2019]// URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/.
3. Massive WannaCry/Wcry Ransomware Attack Hits Various Countries // URL: https://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-various-countries/.
4. Uyazvimosti korporativnykh informatsionnykh sistem, 2019 [Corporate Information Systems Vulnerability]// URL: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/.
5. Gruzdeva, L. M. Model of adaptive information security system of a computer-based data transmission network [Model of a computer-based data transmission network] // Cloud of Science. — 2018. — Т. 3. — № 1.
6. Krupnaya utechka: Operator Wi-Fi v metro Moskvy vykladyvayet dannyye o pol'zovatelyakh v obshchiy dostup [Major leakage: A Wi-Fi operator in the Moscow metro is sharing user data]// URL:https://www.the-village.ru/village/city/situation/308363-krupnaya-utechka-operator-wi-fi-v-metro-moskvy-vykladyvaet-dannye-o-polzovatelyah-v-obschiy-dostup/.
7. Global'noye issledovaniye utechek konfidentsial'noy informatsii v 2018 godu [Global study of confidential information leaks in 2018]// URL: https://www.infowatch.ru/report2018.