УДК 004.056

ЖЕЛЕЗНАЯ ДОРОГА КАК ОБЪЕКТ КИБЕРЗАЩИТЫ

Киселева Е.М.

Российский университет транспорта (МИИТ), Москва, Россия (127994, г. Москва, ул. Образцова, д. 9, стр. 9), e-mail: student.ui.miit@mail.ru

В статье рассмотрены основные предпосылки необходимости обеспечения информационной безопасности и кибербезопасности на железнодорожном транспорте в условиях широкой информатизации и автоматизации транспортных процессов. Главной задачей по обеспечению информационной безопасности ОАО «РЖД» является сохранение способности различных программно-управляемых систем автоматического управления к безопасному и эффективному выполнению функциональных задач в условиях умышленных, целенаправленных воздействий различной физической природы. Автор определил факторы информационной безопасности (хактивизм, информационный терроризм, рост числа целенаправленных компьютерных атак), которые являются решающими при организации современной системы железнодорожных перевозок в России. В статье выделены семь основных направлений обеспечения информационной безопасности и кибербезопасности железнодорожного транспорта, сформулированы цели кибератак на железнодорожных дорогах, а именно кибершпионаж, кибермошенничество, киберхалатность, киберсаботаж и кибердиверсии. В работе приведена статистика атак по мотивам злоумышленников и по методу атак с 2015 г. по 2017 г. Автор представил особенности кибербезопасности объектов ОАО «РЖД», особенности требований кибербезопасности к программно-управляемым системам и комплексам, эксплуатируемым на железной дороге, а также методы противодействия кибератакам, в том числе по программе импортозамещения.

Ключевые слова: информационная безопасность, кибербезопасность, кибератаки, уязвимости, методы противодействия.

RAILWAY AS AN OBJECT OF CYBER SECURITY

Kiseleva E.M.

Russian University of Transport (RUT - MIIT), Moscow, Russia (127994, Moscow, Obrastsova str., 9, bld. 9), e-mail: student.ui.miit@mail.ru

The article considers the basic prerequisites of the need to ensure information security and cyber security in railway transport in the context of wide informatization and automation of transport processes. The main task of ensuring the information security of JSCo «Russian Railways» is to preserve the ability of various program-controlled automatic control systems to safely and efficiently perform functional tasks under the conditions of intentional, targeted actions of various physical nature. The author defined the factors of information security (haktivism, information terrorism, the growth of the number of targeted computer attacks), which are decisive in the organization of a modern rail transportation system in Russia. The article singles out seven main directions for ensuring information security and cyber security of railway transport, formulated the goals of cyber-attacks on railroads, namely cyber espionage, cyber fraud, cybercrimination, cyber-sabotage and cyberdiversions. The statistics of attacks on motives of malefactors and on a method of attacks from 2015 till 2017 are given in the work. The author has presented features of cyber security of objects of Open Society "Russian Railways", features of requirements of cyber-security to program-operated systems and the complexes maintained on the railway, and also counteraction methods cyberattacks, including the import substitution program.

Keywords: information security, cybersecurity, cyberattacks, vulnerabilities, countermeasures.

В последние несколько десятилетий на российских железных дорогах активно шел процесс внедрения программно-аппаратных систем и комплексов для автоматизированного управления техническими объектами и технологическими процессами. Основными целями этого процесса были увеличение эффективности управления вследствие увеличения скорости и уменьшения удельных затрат на перевозки грузов и пассажиров, сокращение численности персонала, снижение уровня аварийности и т.д.

Информационная безопасность [2] и кибербезопасность [4] имеют важное значение в обеспечении безопасности движения в пассажирских и грузовых перевозках, реализации экономических интересов транспортной отрасли России.

Факторы информационной безопасности являются решающими при организации высокоскоростного и скоростного движения и построении интеллектуальных центров и систем управления, особенно учитывая исходящие из киберпространства угрозы потенциальные подверженности информационной инфраструктуры компьютерным атакам.

1. Хактивизм. Развитие этого явления как социального протестного движения и одновременное постепенное превращение отдельных хакеров и хакерских групп в киберпреступные сообщества.

2. Информационный терроризм. Продвижение доктрин кибервойн и создание кибервойск отдельными странами и союзами, например США, Китай, НАТО.

3. Рост числа целенаправленных компьютерных атак (Stuxnet, Flame, Duqu, Gauss, Red October, NetTraveler) на системы управления технологическими процессами важных объектов (вывод из строя энергосистем, объектов ядерной промышленности, других объектов жизнеобеспечения, кражи банковских активов и т. п.) и др.

Основными направлениями обеспечения информационной безопасности и кибербезопасности железнодорожного транспорта (ЖТ), в том числе защита его информационной инфраструктуры (ИИ) от компьютерных атак, являются следующие:

1. Интеграция в единые комплексы автоматизированных систем, связанных с управлением движением поездов, и других автоматизированных информационных и телекоммуникационных систем (АИТС) железнодорожного транспорта.

2. Непрерывное усложнение и совершенствование программного обеспечения и оборудования, используемых в АИТС железнодорожного транспорта.

3. Внедрение практики мониторинга, технического обслуживания и удаленной настройки АИТС, а также серверного и телекоммуникационного оборудования, входящего в состав информационной инфраструктуры железнодорожного транспорта.

4. Противодействие потенциальным нарушителям, разрабатывающим методы использования информационных и телекоммуникационных технологий для нанесения

ущерба, а также попыткам применения этих методов в противоправных целях и конкурентной борьбе.

5. Снижение количества случаев сокрытия попыток или фактического нарушения функционирования АИТС железнодорожного транспорта работниками эксплуатирующих подразделений.

6. Снижение рисков, связанных с временным вынужденным привлечением при создании АИТС, в том числе автоматизированных систем управления технологическими процессами (АСУ ТП), представителей сторонних фирм - производителей и поставщиков программно-аппаратных средств обработки, хранения и передачи информации.

7. Совершенствование законодательной базы, направленной на снижение количества противоправных действий с использованием информационных и телекоммуникационных технологий, в том числе компьютерных атак на железнодорожном транспорте.

Российская железнодорожная транспортная система, как объект, защищаемый от кибератак, представляет собой сложную территориально-распределенную систему, с постоянно меняющимися структурой и параметрами [3]. На данный момент технологическая информационно-коммуникационная сеть ОАО «РЖД» имеет в своем распоряжении более 250 тыс. программно-аппаратных портов для подключения компьютеров и различного рода программно-управляемого оборудования. Для осуществления производственной деятельности используется более 235 тыс. аналого-цифровых радиостанций, 15 тыс. комплектов спутникового связного и навигационного оборудования, более 40 тыс. автоматизированных систем управления посредством микропроцессорной электроники.

Главной задачей по обеспечению информационной безопасности ОАО «РЖД» является сохранение способности различных программно-управляемых систем автоматического управления к безопасному и эффективному выполнению функциональных задач в условиях умышленных, целенаправленных воздействий различной физической природы.

Объектами кибератак на железнодорожных дорогах могут быть системы диспетчерской и электрической централизации, которые обеспечивают формирование безопасного маршрута движения поездов, системы защиты и регулирования энергоснабжения, а также обслуживающий персонал (диспетчеры, дежурные).

Цели кибератак:

– Кибершпионаж – получение секретной или конфиденциальной информации без разрешения владельцев данной информации.

– Кибермошенничество – взлом системы с целью причинения материального или иного ущерба путем получения информации.

– Киберхалатность – кибератаки из-за человеческой непреднамеренной ошибки.

– Киберсаботаж – снижение пропускной способности и скорости перевозок вплоть до полной остановки движения железнодорожного транспорта.

– Кибердиверсии – преднамеренное создание опасных маршрутов следования.

Нарушители, злоумышленники, осуществляющие кибератаки: конкуренты, спецслужбы, организованные преступные группировки, хакеры, вооруженные силы иностранных государств (кибервойска) [1, 6]. При этом финансовая выгода для злоумышленников является важнейшим мотивом совершения кибератак (рис. 1).

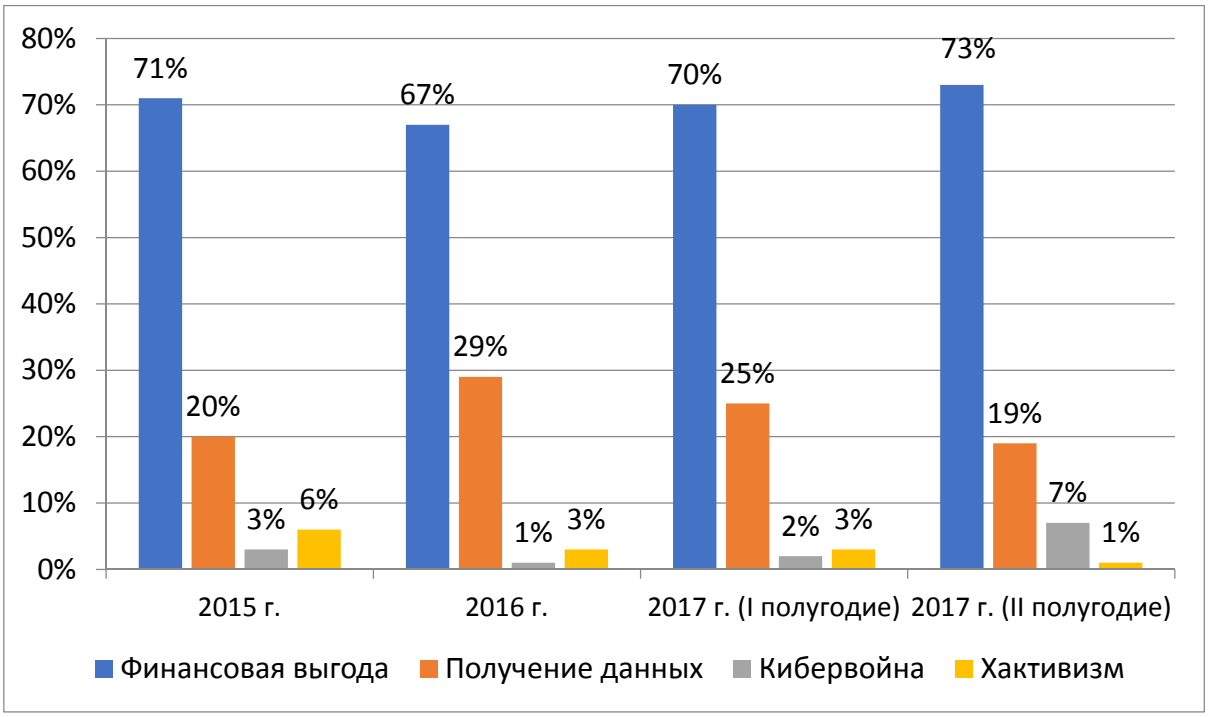

Рис. 1. Статистика атак (по мотивам злоумышленников)

Уровень технической оснащенности и компетентности (информационной осведомленности) злоумышленника может быть довольно высоким, например, могут использоваться вредоносное программное обеспечение [5], заранее размещенные программно-аппаратные «закладки» (рис. 2).

Рис. 2. Статистика атак (по методу атак)

Особенности кибербезопасности объектов ОАО «РЖД»

Реализация требований кибербезопасности к программно-управляемым системам и комплексам, эксплуатируемым на железной дороге, имеет специфические особенности, представленные на рис. 3.

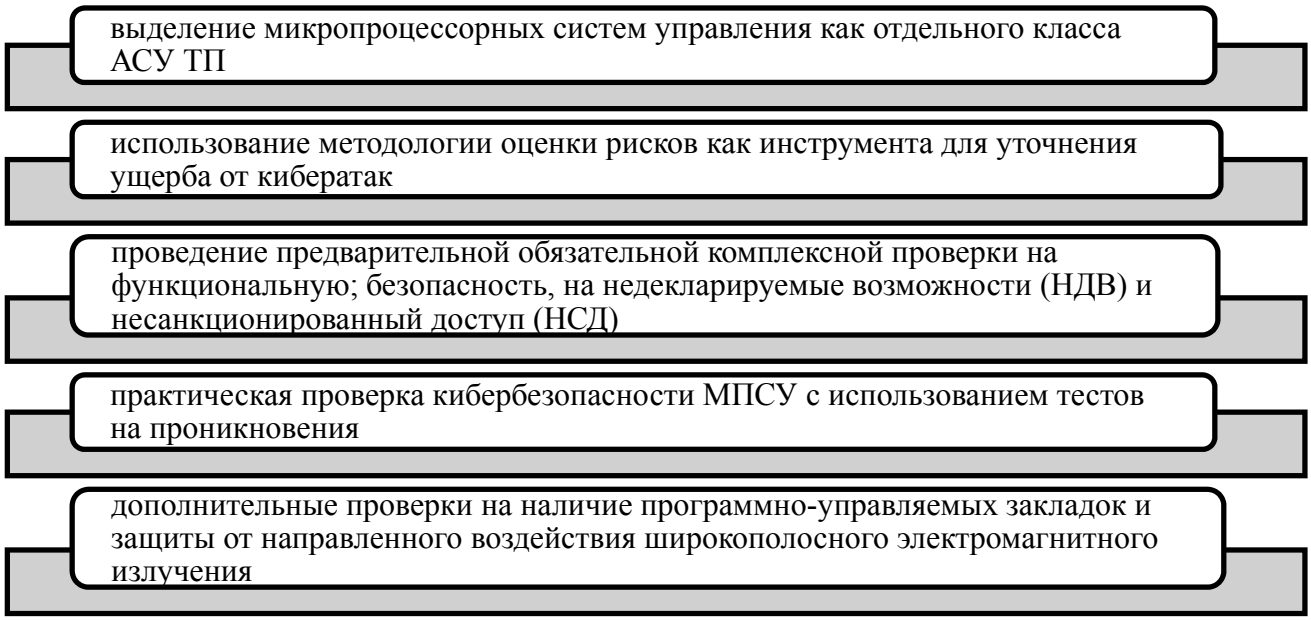

Рис. 3. Особенности требований кибербезопасности к программно-управляемым системам и комплексам, эксплуатируемым на железной дороге

В процессе проведения испытаний на кибербезопасность выявляются недостатки используемого типового и прикладного программного обеспечения (рис. 4).

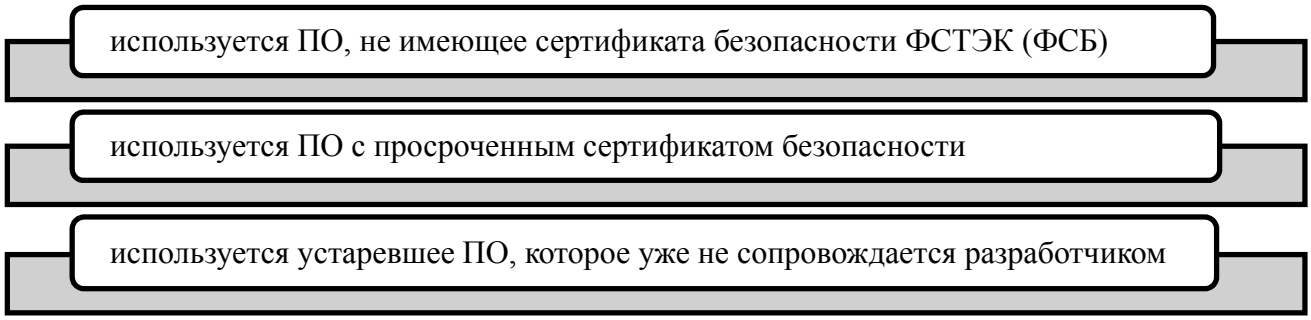

Рис. 4. Недостатки используемого на железной дороге типового и прикладного программного обеспечения

Комплекс методов защиты от кибератак представлен на рис. 5.

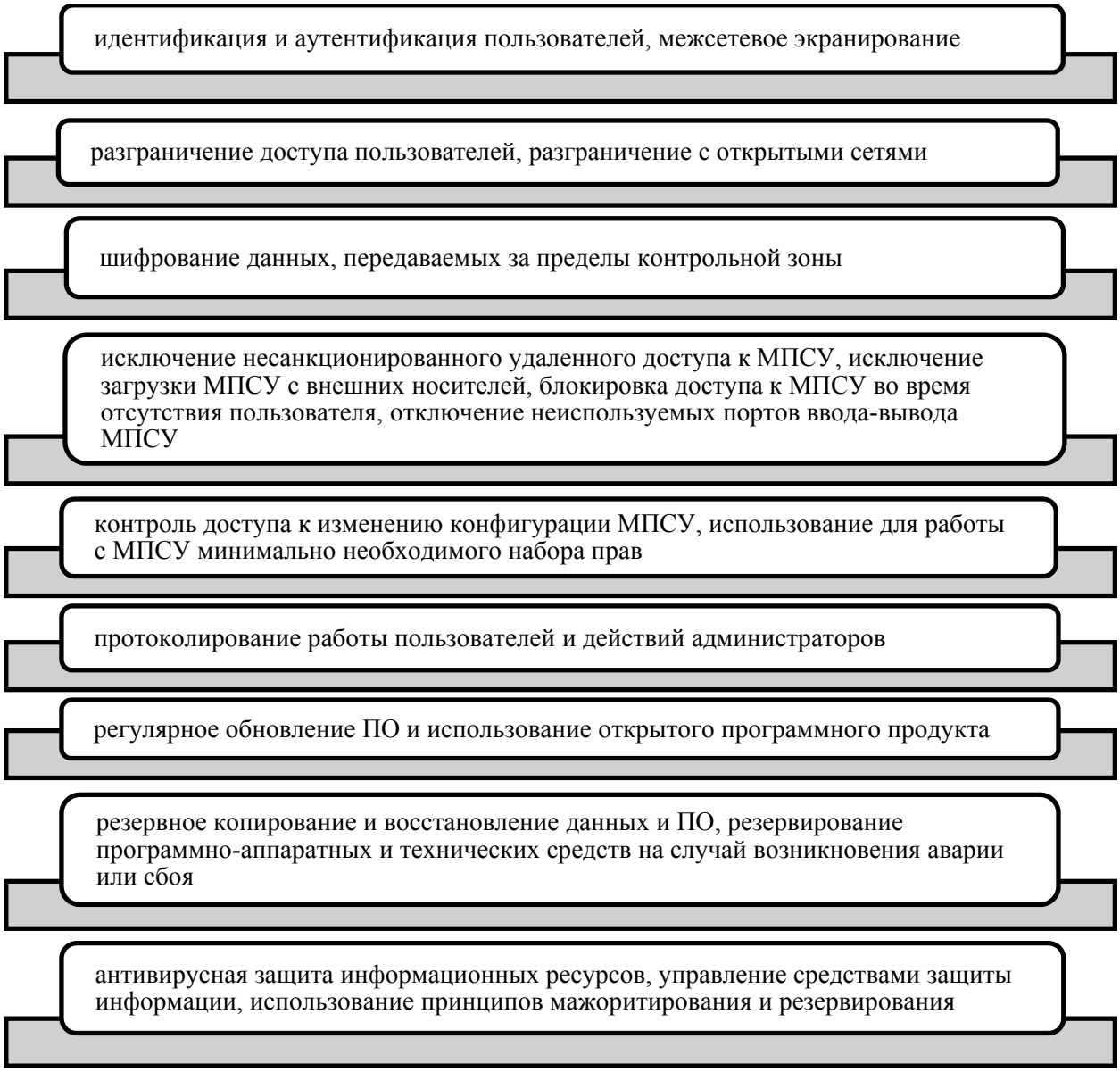

Рис. 5. Методы противодействия кибератакам

На рис. 6 представлены методы противодействия с помощью программы импортозамещения.

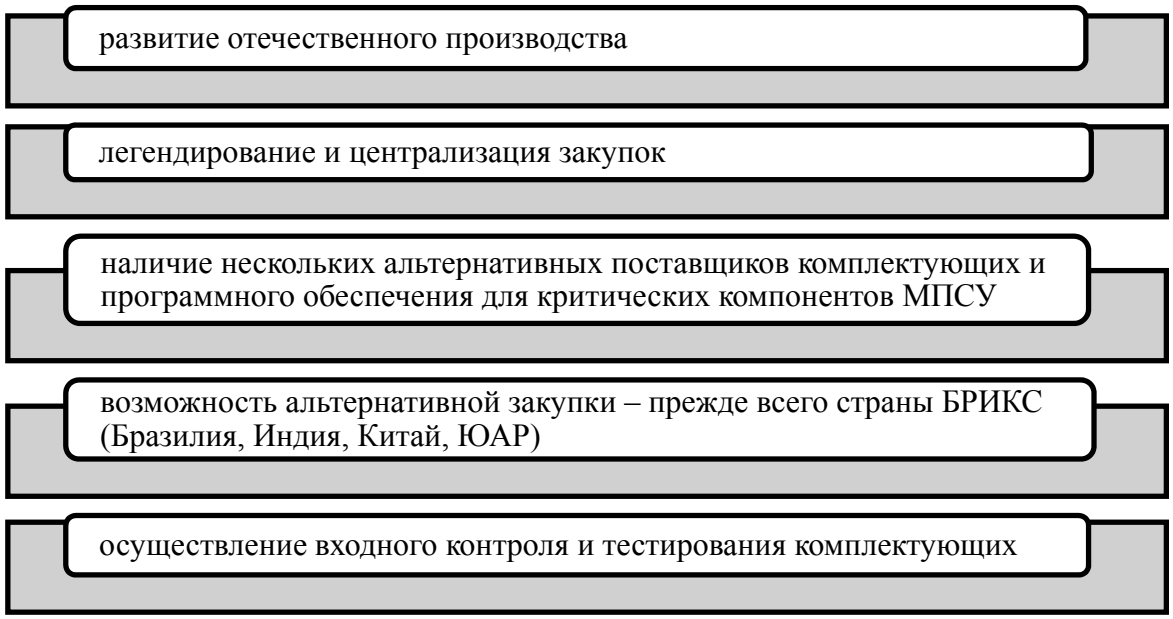

Рис. 6. Методы противодействия кибератакам по программе импортозамещения

Каждая вторая крупная организация обнаруживает следы присутствия злоумышленников в своей инфраструктуре. При этом среднее время присутствия злоумышленника в инфраструктуре составляет примерно три года.

На общую статистику влияют два момента: во-первых, в информационном пространстве увеличилось число высококвалифицированных и технологически оснащенных кибергруппировок, а во-вторых, государственная политика в области информационной безопасности все больше требует от владельцев информационных инфраструктур выстраивать корректные процессы по выявлению, реагированию и локализации компьютерных инцидентов с использованием правильных технологий.

Для обеспечения безопасности корпоративной системы необходим комплексный подход. Без учета всех компонентов функционирующей системы невозможно создать защищенную инфраструктуру. Векторы атак на корпоративные инфраструктуры компаний со стороны внешних сетей и со стороны внутреннего нарушителя основывались на эксплуатации распространенных уязвимостей и недостатков, для устранения которых, как правило, достаточно применить самые общие принципы обеспечения информационной безопасности. Необходимо особое внимание уделять строгости парольной политики, защите привилегированных учетных записей, а также защите от атак на публичные веб-приложения. Необходимо обеспечить регулярное обновление используемого ПО и установку актуальных обновлений безопасности на автоматизированной основе.

Литература

1. Актуальные киберугрозы — 2017. Тренды и прогнозы [Электронный ресурс] // Positive Technologies. – 2017. – 21 с. // URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Corporate-vulnerabilities-2018-rus.pdf (дата обращения: 02.08.18).

2. Груздева Л. М. Основы информационной безопасности: учеб. пособие/ Л.М. Груздева. - М.: Юридический институт МИИТа, 2018. - 101 с.

3. Кибербезопасность российских железных дорог [Электронный ресурс] // itWeek.ru: сайт. – URL: https://www.itweek.ru/security/article/detail.php?ID=183893 (дата обращения: 02.08.18).

4. Макаров Б.А. Актуальность кибербезопасности на железнодорожном транспорте // Техника железных дорог. – 2015. – № 3 (31). – С. 19 – 24 // URL: http://tb-inform.ru/wp-content/uploads/2016/03/Statya-ZHT.pdf (дата обращения: 02.08.18).

5. Монахов, Ю.М. Вредоносные программы в компьютерных сетях: учеб. пособие / Ю.М. Монахов, Л.М. Груздева, М.Ю. Монахов; Владим. гос. ун-т. - Владимир: Изд-во Владим. гос. ун-та, 2010. – 72 с.

6. Уязвимости корпоративных информационных систем [Электронный ресурс] // Positive Technologies. – 2018. – 21 с. // URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Corporate-vulnerabilities-2018-rus.pdf (дата обращения: 02.08.18).