

КИБЕРУГРОЗЫ: ПРИЧИНЫ ВОЗНИКНОВЕНИЯ И РЕКОМЕНДАЦИИ ПО ПРЕДУПРЕЖДЕНИЮ*

Евгений Юрьевич ХРУСТАЛЁВ^а, Глеб Андреевич КОСТЮРИН^б

^а доктор экономических наук, профессор, заведующий лабораторией,
Центральный экономико-математический институт РАН, Москва, Российская Федерация
stalev777@yandex.ru
ORCID: отсутствует
SPIN-код: 1618-1843

^б студент факультета национальной безопасности Института права и национальной безопасности,
Российская академия народного хозяйства и государственной службы при Президенте РФ,
Москва, Российская Федерация
g.kostyurin@yandex.ru
ORCID: отсутствует
SPIN-код: отсутствует

* Ответственный автор

История статьи:

Получена 21.03.2019
Получена в доработанном
виде 10.04.2019
Одобрена 25.04.2019
Доступна онлайн
17.06.2019

УДК 004.942

JEL: F52, H56, J28, M15,
N10

Ключевые слова:

кибербезопасность,
информационная
безопасность, киберугроза,
кибератака,
киберпреступление

Аннотация

Предмет. Статья посвящена проблемам незащищенности информационной инфраструктуры от кибератак. Актуальность работы вызвана неуклонным ростом киберпреступлений, наносящих ущерб не только гражданам и организациям, но и экономике нашей страны. Существует множество неразрешенных проблем, касающихся не только обеспечения должного уровня защиты от разных видов киберугроз, но и несовершенства законодательства, а также отсутствия единого системного подхода к данному вопросу.

Цели. Анализ и систематизация хронологии крупнейших кибератак за последнее время, разработка классификации киберпреступлений и их последствий, определение основных рекомендаций по предупреждению киберпреступлений и совершенствованию уровня кибербезопасности в условиях глобальной цифровизации.

Методология. В работе использованы методы системного анализа, сравнительного, структурного и логического анализа, эконометрический анализ, контент-анализ СМИ, экономико-статистические методы и моделирование.

Результаты. Систематизирована хронология крупнейших кибератак, разработана классификация киберпреступлений и их последствий. Определены основные рекомендации по совершенствованию уровня кибербезопасности в условиях глобальной цифровизации.

Выводы. Исследованы основные понятия, описаны формы и виды кибератак, рассмотрены крупнейшие мировые кибератаки. Проанализированы основные причины возникновения киберпреступлений и сделаны конкретные рекомендации по их предупреждению.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2019

Для цитирования: Хрусталёв Е.Ю., Костюрин Г.А. Киберугрозы: причины возникновения и рекомендации по предупреждению // Национальные интересы: приоритеты и безопасность. – 2019. – Т. 15, № 6. – С. 1185 – 1194. <https://doi.org/10.24891/ni.15.6.1185>

Введение

С каждым годом жизнь современного человека становится все более совершенной в связи с влиянием на нее различных

технологий. Уже не нужно беспокоиться о том, как расплатиться в магазине, забыв наличные деньги, – достаточно просто приложить телефон к терминалу, и денежные средства моментально спишутся с вашего

банковского счета, не нужно помнить или записывать в блокнот все свои логины и пароли от учетных записей в электронных ресурсах – браузер сам запомнит их и подскажет в нужный момент.

Чем шире человек использует IT-технологии, чем проще и удобнее становится его жизнь, тем больше он становится IT-зависимым и тем выше становятся риски причинения вреда его жизни в случае разрушения системы. Ведь пока не было автомобилей и самолетов, невозможно было попасть в дорожно-транспортное происшествие или в авиакатастрофу.

На данный момент число устройств, подключенных к сети Интернет, составляет 10 млрд шт., а согласно прогнозам, к 2020 г. эта цифра будет достигать 50 млрд.

Российские исследователи А.Е. Бобылев и А.В. Трофимова в своей работе утверждают, что технологии в наше время позволяют подключаться к сети Интернет многим вещам таким образом, что из полученного арсенала датчиков, бытовых приборов и других предметов, имеющих активное подключение к сети, можно собрать сложную систему, выполняющую команды устройства управления, роль которых может выполнять любой гаджет – телефон, планшет, ноутбук [1].

Интернет вещей (*IoT*) – это концепция пространства, в котором все компоненты из аналогового и цифрового миров могут быть совмещены: это переопределяет наши отношения с объектами, а также свойства и суть самих объектов. Интернет вещей позволяет загружать свои данные в облачные системы и обратно, создавая значительные возможности как для пользователей, использующих данные технологии, так и для хакеров, ставящих своей целью кражу данных. Наиболее существенная особенность IoT – это возможность IoT-устройства взаимодействовать с внешней средой. При этом Ю.В. Гольчевский и Н.А. Филимонова отмечают, что от

безопасности и надежности функционирования таких устройств может зависеть физическая безопасность и жизни людей [2].

За последние 10 лет количество вредоносных программ увеличилось в 70 раз. Общемировой экономический ущерб от киберпреступлений составил около 1 трлн долл. США, что является примерно 1/7 ущерба от всех стихийных бедствий на планете.

Обзор научных исследований по данной тематике

Актуальное положение дел, статистические данные и возможные риски в сфере кибербезопасности в условиях цифровой трансформации подробно изучены в статьях отечественных и зарубежных авторов¹ [3, 4]. В частности, предполагается, что в ближайшие 5–7 лет от 9 до 21 трлн долл. США глобальных экономических ценностей могут оказаться под угрозой, если международные организации и государства не создадут успешной стратегии борьбы с киберугрозами. Для выработки соответствующей стратегии необходимо не только выполнять теоретические исследования с использованием математического аппарата, но и успешно применять прикладные методики защиты уязвимых систем, содержащиеся в работах российских авторов (в частности А.Г. Полетыкина², Н.О. Андреева [5]), в том числе средства и методы

¹ Пацация С.Б. Проблемы кибер-рисков в современности: материалы международной научно-практической конференции «Новая наука как результат инновационного развития общества». Уфа: ООО «Агентство международных исследований», 2017. С. 111–113; Саблукова Ю.Г. Классификация кибер-рисков в эпоху цифровой экономики: материалы XIX международной научно-практической конференции «Страхование в эпоху цифровой экономики: проблемы и перспективы». Йошкар-Ола: Изд-во МарГУ, 2018. С. 87–91; Semenova K.D., Tarasova K.I. Statistical Research of Global Cyber-Risks: The Cost of Cyber-Crime. In: Topical Questions of Contemporary Science: Collection of Scientific Articles. Aspekt Publishing, Taunton, MA, United States of America, 2017, pp. 315–320.

² Полетыкин А.Г. Методика оценки киберустойчивости: материалы VII международной конференции «Управление развитием крупномасштабных систем». М.: Институт проблем управления им. В.А.Трапезникова РАН, 2013. С. 193–200.

^{*} Статья подготовлена при финансовой поддержке РФФИ, грант № 18-00-00177 (18-00-00164).

криптографической защиты информации, описанные в работе М.Н. Гришина³.

Для выявления причин возникновения угроз и выработки алгоритмов противодействия кибератакам В.Ф. Турыгина, В.Ф. Форд в своей работе [6] предлагают использование технологий машинного обучения – эффективного инструмента, который может быть использован во многих областях информационной безопасности. Машинное обучение может быть успешно использовано для разработки систем аутентификации, оценки безопасности доказательств человеческого взаимодействия, смарт-профилирования данных и т.д.

В работе И.М. Глотиной одной из главных причин роста киберпреступности как теневого бизнеса называется незначительный риск: поскольку киберпреступность не имеет границ, правоохранительным органам трудно ловить преступников, а проведение международных расследований и ведение судебных дел обходятся в значительные средства. Подобные действия, как правило, предпринимаются только в особых случаях [7].

В Доктрине информационной безопасности РФ под информационной безопасностью понимается 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 государства⁴. В работе И.В. Беловой информационная безопасность понимается как состояние сохранности

информационных ресурсов, баз данных и защищенность законных прав личности, общества и государства в информационной сфере [8].

В то же время В.Е. Кадулин, Е.Н. Клочкова [9] считают, что термин «кибербезопасность» (*cyber security*) частично совпадает с понятием «информационная безопасность» (*information security*), но подразумевает возможность проведения компьютерных атак на информационную инфраструктуру противодействующей стороной. Существует много подходов к определению понятия «кибербезопасность». Например, А.С. Алпеев предлагает следующее определение: кибербезопасность – раздел безопасности, изучающий процессы формирования, функционирования и эволюции киберобъектов в целях выявления источников киберопасности, которые могут нанести им ущерб, и формирования законов и других нормативных актов, регламентирующих термины, требования, правила, рекомендации и методики, выполнение которых должно гарантировать защищенность киберобъектов от всех известных и изученных источников киберопасности [10].

В свою очередь, в компании Cisco⁵ считают, что кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак, которые обычно направлены на получение доступа к конфиденциальной информации, ее изменение и уничтожение, на вымогательство у пользователей денег или на нарушение нормальной работы компаний.

Мы предложим свой вариант определения данного понятия. *Кибербезопасность – это один из разделов информационной безопасности, который означает состояние сохранности и защищенности сетей, компьютеров, программного обеспечения, сетевых устройств, баз данных, законных*

³ Гришин М.Н. Кибербезопасность. Средства и методы криптографической защиты информации: материалы XIX региональной научно-практической конференции «Молодежь XXI века: шаг в будущее». Благовещенск: Амурский государственный университет, 2018. С. 175–176.

⁴ Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646. URL: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>

⁵ Cisco – американская транснациональная компания, разрабатывающая и продающая сетевое оборудование, предназначенное в основном для крупных организаций и телекоммуникационных предприятий.

прав личности, общества и государства в цифровой сфере.

Формы и особенности современных кибератак

Кибератака – это покушение на информационную безопасность компьютерной системы. Выделим следующие формы кибератак.

Кибертерроризм. Финансируется заинтересованными организациями, государствами и включает крупномасштабные мероприятия, направленные на получение секретных данных или нарушение функционирования ключевых систем крупных организаций или государств.

Киберрэккет. Финансируется заинтересованными организациями либо из собственных источников. Совершается в целях кражи данных, нарушения функционирования системы, шифрования и требования выкупа за возобновление работы системы.

Бытовые кибератаки. Чаще всего финансируются из собственных или заемных источников. Как правило, это мелкое мошенничество, осуществляемое в целях кражи денежных средств с банковской карты, кражи личных данных для получения информации об объекте кибератаки, либо в целях получения выкупа.

Последствия кибератак ежегодно исчисляются миллиардами долларов. Выделяют следующие виды последствий кибератак.

Кража конфиденциальной информации. Утечка данных, содержащих информацию о патентах, технологиях, поставщиках, контрагентах, данных, являющихся коммерческой тайной, интеллектуальной собственностью субъекта.

Ущерб репутации. Факт успешной совершенной кибератаки формирует негативный образ уязвимой компании, с которой небезопасно вступать в сотрудничество.

Мошенничество. Непосредственная кража материальных ресурсов организации посредством доступа к банковским счетам или имуществу объекта кибератаки.

Судебные разбирательства. Разбирательства в суде неминуемо приведут к существенным расходам в связи с рассмотрением и разрешением судебного дела.

Упущенная выгода. Блокировка информационных систем компании неизбежно ведет к торможению всех бизнес-процессов и к снижению эффективности основной деятельности объекта кибератаки.

Наиболее популярными видами кибератак в 2016 г. были следующие⁶:

- атаки на web-приложения (SQL-инъекции/XSS) – 24%;
- внедрение вредоносного кода – 19%;
- атаки на приложения – 19%;
- DDoS/DDoS-атаки (перегрузка сервера большим числом запросов) – 9%;
- разведывательные атаки: активные (поиск конфиденциальной информации в системе жертвы) либо пассивные (поиск конфиденциальной информации вне системы жертвы) – 9%;
- остальные виды атак – 20%.

Распространение вредоносных вирусов

Одним из самых заметных вирусов, распространяемых по электронной почте, в 1999 г. стал вирус Melissa – первый вредоносный код, который нарушил работу почтовых серверов многих крупных компаний мира. Вирус распространялся волнообразно, создавая огромный поток инфицированных писем. Ущерб от этой «эпидемии» оценивают в 80 млн долл. США⁷.

⁶ Кибератаки / TADVISER. Государство. Бизнес. ИТ.
URL: <http://tadviser.ru/index.php/Статья:Кибератаки>

⁷ Топ-10 компьютерных вирусов.
URL: <http://star-force.ru/press/articles/?news=2955>

Одна из первых масштабных DDoS-атак была совершена в 2000 г. посредством вируса Mafiaboy. Атака была инициирована канадским школьником, объектом стали несколько популярных сайтов, включая Amazon, Dell, Yahoo, Fifa.com, eBay и CNN. Ущерб оценили примерно в 1,2 млрд долл. США. Среди отечественных исследований DDoS-атаки подробно изучены в работах Е.А. Гавриловой [11] и М.Д. Зеленского⁸.

Первым вирусом, оказывающим воздействие на мобильные устройства, был Cabir, появившийся в 2004 г. На экранах телефонов, зараженных данным вирусом, высвечивалась надпись *Caribe*. Вирус был замаскирован под ПО для защиты мобильных устройств от вирусов – Caribe Security Manager, которую пользователь должен был установить самостоятельно.

Первым вирусом, распространяемым через социальные сети, стал Zeus. Началось заражение в 2007 г. путем рассылки в социальной сети Facebook фото со ссылкой на веб-сайт, содержащий троянскую программу. Эта программа внедрялась в систему, добывая злоумышленникам регистрационные данные пользователя, позволявшие похищать средства со счетов клиентов ведущих европейских банков. Кибератака затронула пользователей Италии, Германии, Нидерландов и Испании⁹.

Самым известным вирусом, поражающим системы управления производственными процессами, стал Stuxnet. Данный вирус – это первое в мире использованное в военных целях кибероружие, которое в 2009 г. вывело из строя 1 368 ядерных центрифуг в Иране, разрушив всю их инфраструктуру, что отбросило ядерную программу Ирана на годы назад.

⁸ Зеленский М.Д. Ddos-атаки: типы атак, устранение Ddos-атак: материалы IV Всероссийской научно-технической конференции «Студенческая наука для развития информационного общества». Ставрополь: Северо-Кавказский федеральный университет, 2016. С. 241–243.

⁹ 10 главных кибератак в истории человечества. URL: <https://vedomosti.ru/technology/galleries/2017/10/26/739471-10-glavnih-kiberatak>

Широкую известность получил вирус Lazarus, который в 2014 г. привел к массовой утечке личных данных из электронной почты работников компании Sony Pictures, а также неизданных фильмов киностудии. Ущерб компании оценен в 100 млн долл. США.

В 2016 г. на российские информационные ресурсы было совершено более 50 млн кибератак – это в три раза больше, чем в 2015 г. Более 60% атак производится из-за границы, с территории иностранных государств. Так, в первой половине 2017 г. были выявлены две крупные эпидемии вирусов шифровальщиков-вымогателей – WannaCry и NotPetya/ExPetr. Общий ущерб от последствий только этих двух крупных эпидемий оценивают более чем в 1 млрд долл. США.

Вредоносная программа WannaCry была детально проанализирована Н.Е. Кувшиновым, А.А. Галютдиновым [12]. Вирус атаковал 200 тыс. компьютеров, серьезные убытки понесли 150 стран. Он проникал в компьютеры с операционной системой Windows с устаревшими обновлениями, взламывал и зашифровывал жесткие диски и требовал 300 долл. за разблокировку системы. Воздействию вируса подверглись не только компьютеры и мобильные устройства частных лиц и организаций, но и объектов критической инфраструктуры – больниц, в которых были заблокированы различные устройства, включая медицинское оборудование. Кроме того, некоторым заводам пришлось остановить производство в связи с зашифрованным производственным оборудованием.

При этом самой дорогостоящей кибератакой является отнюдь не эпидемия WannaCry, а эпидемия шифровальщика NotPetya, также известного как ExPetr. Его принцип действия был схожим – проникновение, шифрование и требование выкупа. Однако в отличие от WannaCry, жертвами NotPetya стали организации, поскольку у создателей данного вируса был доступ к центру обновлений

финансового программного обеспечения MeDoc, которое хозяйствующие субъекты использовали в своей деятельности¹⁰.

Рекомендации по предупреждению киберпреступлений

Для предупреждения большинства кибератак на уровне личности необходимо соблюдать основные меры безопасности при работе в информационной среде.

Для защиты от социальной инженерии Р.А. Маслов предлагает следующее¹¹:

- иметь два почтовых ящика – личный, используемый для персональной корреспонденции, и публичный, используемый для регистрации на различных порталах;
- не переходить по ссылкам в письмах, полученных от неизвестных источников;
- не отвечать на спам;
- своевременно обновлять браузер;
- использовать специальные антифишинговые и спам-фильтры при работе в Интернете.

Для защиты от вредоносного ПО необходимо также:

- позаботиться о том, чтобы на компьютере или мобильном устройстве был установлен антивирус. Хотя даже самые совершенные антивирусные программы блокируют лишь 40% атак, это и есть самые распространенные угрозы;
- постоянно обновлять ПО устройства до максимальной версии потому, что зачастую злоумышленники используют уязвимости в устаревшем коде, вследствие чего разработчики постоянно выявляют их и выпускают обновления;

– регулярно осуществлять резервное копирование всех данных как в облачное хранилище, так и на физический носитель;

– составлять сложные пароли для учетных записей, не состоящие из общедоступной информации (дата рождения, номер телефона, ФИО), кроме того, необходима полная смена паролей от всех учетных записей не реже раза в месяц;

– в банковских и почтовых сервисах применять двухфакторную аутентификацию.

Обычно в организациях более 60% инцидентов в сфере информационной безопасности связано с внутренними нарушениями. Технологии защиты от внутренних угроз информационной безопасности подробно раскрыты в статье А.Е. Сулавко [13]. Большинство из них связано с социальной инженерией. Неосведомленный работник является потенциальным нарушителем и источником возникновения угрозы. Для предотвращения внутренних нарушений в организации необходимо внедрение специальной системы обучения и контроля знаний по информационной безопасности. Сотрудникам отдела информационной безопасности необходимо донести до работников ключевые сведения о потенциальных угрозах, выдать соответствующие информационно-справочные материалы и провести инструктаж.

В настоящее время в вопросах информационной безопасности распространяется проактивная и другие виды защиты информационных ресурсов [14, 15]. Для борьбы с киберпреступниками специалистам необходимо опережать хакеров по уровню знаний, разрабатывать превентивные методы защиты программного обеспечения, заранее искать и устранять потенциальные уязвимости в защищаемых системах¹².

¹⁰ 5 самых выдающихся кибератак. URL: <https://kaspersky.ru/blog/five-most-notorious-cyberattacks/21607>

¹¹ Маслов Р.А. Социальная инженерия в кибер-информационном пространстве и меры защиты от нее: материалы XI международной научно-практической конференции «Наука и образование: отечественный и зарубежный опыт». Белгород: ООО ГиК, 2018. С. 245–250.

¹² Информационная и кибербезопасность. URL: <https://yandex.ru/profi/courses2018/cybersecurity>

Список литературы

1. Бобылёв А.Е., Трофимова А.В. Проблема защиты данных в интернете вещей // *Nauka-Rastudent.ru*. 2016. № 3. С. 25. URL: <http://nauka-rastudent.ru/27/3279/>
2. Гольчевский Ю.В., Филимонова Н.А. Подход к обнаружению вредоносной активности в интернете вещей // *Информация и безопасность*. 2017. Т. 20. № 3. С. 464–467.
3. Вяткин А.А. Экономическая безопасность электронных платежных систем: снижение киберрисков в условиях цифровой трансформации // *Инновационное развитие экономики*. 2018. № 5. С. 295–298.
4. Alosaimi R., Alnuet M. Risk Management Frameworks for Cloud Computing: A Critical Review. *International Journal of Computer Science & Information Technology*, 2016, vol. 8, iss. 4. URL: <https://doi.org/10.5121/ijcsit.2016.8401>
5. Андреев Н.О. Формирование и развитие угроз в информационных системах // *Прикладная информатика*. 2006. № 6. С. 87–100.
6. Турыгина В.Ф., Форд В.Ф., Матвеевнина А.И. Применение машинного обучения в кибер-безопасности // *Научный альманах*. 2017. № 6-1. С. 405–408.
7. Глотина И.М. Киберпреступность как теневой бизнес // *Вестник Челябинского государственного университета*. 2016. № 6. С. 51–57.
8. Белова И.В. Формулировка понятия «информационная безопасность» в учебном курсе дисциплины «Основы информационной безопасности» // *Психология, социология и педагогика*. 2011. № 3. URL: <http://psychology.snauka.ru/2011/12/74>
9. Кадулин В.Е., Клочкова Е.Н. Соотношение понятий «кибербезопасность» и «информационная безопасность» в современном правовом поле // *Вопросы кибербезопасности*. 2017. № S2. С. 7–10.
10. Алтеев А.С. Терминология безопасности: кибербезопасность и информационная безопасность // *Вопросы кибербезопасности*. 2014. № 5. С. 39–42.
11. Гаврилова Е.А. Исследование методов обнаружения сетевых атак // *Научные записки молодых исследователей*. 2017. № 4. С. 55–58. URL: <https://cyberleninka.ru/article/v/issledovanie-metodov-obnaruzheniya-setevyh-atak>
12. Кувшинов Н.Е., Галаутдинов А.А. Анализ вредоносной программы WannaCry // *Форум молодых ученых*. 2017. № 9. С. 499–503.
13. Сулавко А.Е. Технологии защиты от внутренних угроз информационной безопасности // *Вестник Сибирской государственной автомобильно-дорожной академии*. 2011. № 1. С. 45–51. URL: <https://cyberleninka.ru/article/v/tehnologii-zaschity-ot-vnutrennih-ugroz-informatsionnoy-bezopasnosti>
14. Хрусталёв Е.Ю., Елизарова М.И. Концептуальные основы построения системы информационной безопасности производственного предприятия // *Политематический сетевой электронный научный журнал КубГАУ*. 2017. № 6. С. 107–127. URL: <http://ej.kubagro.ru/2017/06/pdf/07.pdf>

15. Иванова Е.И., Хрусталёв Е.Ю. Информатизация государственного управления и проблемы национальной безопасности // *Национальные интересы: приоритеты и безопасность*. 2008. Т. 4. Вып. 2. С. 70–78. URL: <https://cyberleninka.ru/article/v/informatizatsiya-gosudarstvennogo-upravleniya-i-problemy-natsionalnoy-bezopasnosti>

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

CYBERSECURITY THREATS: TRIGGERS AND PREVENTION RECOMMENDATIONS

Evgenii Yu. KHRUSTALEV ^{a,*}, Gleb A. KOSTYURIN ^b

^a Central Economics and Mathematics Institute of Russian Academy of Sciences (CEMI RAS),
Moscow, Russian Federation
stalev777@yandex.ru
ORCID: not available

^b Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russian Federation
g.kostyurin@yandex.ru
ORCID: not available

* Corresponding author

Article history:

Received 21 March 2019
Received in revised form
10 April 2019
Accepted 25 April 2019
Available online
17 June 2019

JEL classification: F52, H56,
J28, M15, N10

Keywords: cybersecurity,
information security, cyber
threat, cyber attack,
cybercrime

Abstract

Subject The article focuses on issues of the exposure of IT infrastructure to cyber attacks as the global community sees an increasing number of cybercrimes.

Objectives The study analyzes and systematized major cyber attacks, which have taken place recently, chronologically. We classify cybercrimes and their consequences, define new recommendations for preventing cybercrimes and improving the cybersecurity level during the global digitization.

Methods Research is based on methods of a systems analysis, comparative, structural and logic analysis, econometric analysis, content-analysis, mass media, economic-statistical methods and modeling.

Results We arranged major cybersecurity attacks chronologically, classified cybercrimes and their consequences. The article provides the main recommendations for improving the cybersecurity level during the global digitization.

Conclusions and Relevance We reviewed key concepts, described forms and types of cyber attacks and focus on global ones. The article also analyzes key triggers of cybercrimes and gives specific recommendations for preventing them.

© Publishing house FINANCE and CREDIT, 2019

Please cite this article as: Khrustalev E.Yu., Kostyurin G.A. Cybersecurity Threats: Triggers and Prevention Recommendations. *National Interests: Priorities and Security*, 2019, vol. 15, iss. 6, pp. 1185–1194.
<https://doi.org/10.24891/ni.15.6.1185>

Acknowledgments

The article was supported by the Russian Foundations for Basic Research, grant № 18-00-00177(18-00-00164).

References

1. Bobylev A.E., Trofimova A.V. [Data protection problem on the Internet of Things]. *Nauka-Rastudent.ru*, 2016, no. 3, p. 25. (In Russ.) URL: <http://nauka-rastudent.ru/27/3279/>
2. Gol'chevskii Yu.V., Filimonova N.A. [An approach to detecting malicious activity on the Internet of Things]. *Informatsiya i bezopasnost' = Information and Security*, 2017, vol. 20, no. 3, pp. 464–467. (In Russ.)
3. Vyatkin A.A. [Economic security of electronic payment systems: Mitigation of cybersecurity risks during the time of digital transformation]. *Innovatsionnoe razvitie ekonomiki = Innovative Development of Economy*, 2018, no. 5, pp. 295–298. (In Russ.)

4. Alosaimi R., Alnuem M. Risk Management Frameworks for Cloud Computing: A Critical Review. *International Journal of Computer Science & Information Technology*, 2016, vol. 8, iss. 4. URL: <https://doi.org/10.5121/ijcsit.2016.8401>
5. Andreev N.O. [Emergence and growth of threats in IT systems]. *Prikladnaya informatika = Applied Informatics*, 2006, no. 6, pp. 87–100. (In Russ.)
6. Turygina V.F., Ford V.F., Matvevnina A.I. [The use of machine learning in cybersecurity]. *Nauchnyi al'manakh = Science Almanac*, 2017, no. 6-1, pp. 405–408. (In Russ.)
7. Glotina I.M. [Cybercrime as a shadow business]. *Vestnik Chelyabinskogo gosudarstvennogo universiteta = Bulletin of Chelyabinsk State University*, 2016, no. 6, pp. 51–57. (In Russ.)
8. Belova I.V. [The formulation of the concept 'information security' in the training course of the discipline "Fundamentals of information security"]. *Psikhologiya, sotsiologiya i pedagogika = Psychology, Sociology and Pedagogy*, 2011, no. 3. URL: <http://psychology.snauka.ru/2011/12/74> (In Russ.)
9. Kadulin V.E., Klochkova E.N. [The relation between the concepts of information security and cyber security in the contemporary legal environment]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2017, no. S2, pp. 7–10. (In Russ.)
10. Alpeev A.S. [Terminology of security: Cybersecurity, information security]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2014, no. 5, pp. 39–42. (In Russ.)
11. Gavrilova E.A. [Research methods for detecting network attacks]. *Nauchnye zapiski molodykh issledovatelei = Scientific Notes of Young Scientists*, 2017, no. 4, pp. 55–58. URL: <https://cyberleninka.ru/article/v/issledovanie-metodov-obnaruzheniya-setevykh-atak> (In Russ.)
12. Kuvshinov N.E., Galyautdinov A.A. [Analysis of the malware WannaCry]. *Forum molodykh uchenykh = Forum of Young Scientists*, 2017, no. 9, pp. 499–503. (In Russ.)
13. Sulavko A.E. [Technologies of protection against internal threats of information security]. *Vestnik Sibirskoi gosudarstvennoi avtomobil'no-dorozhnoi akademii = The Russian Automobile and Highway Industry Journal*, 2011, no. 1, pp. 45–51. URL: <https://cyberleninka.ru/article/v/tehnologii-zaschity-ot-vnutrennih-ugroz-informatsionnoy-bezopasnosti> (In Russ.)
14. Khrustalev E.Yu., Elizarova M.I. [Conceptual foundations formation of information security system for a production enterprise]. *Politematicheskii setevoi elektronnyi nauchnyi zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta*, 2017, no. 6, pp. 107–127. (In Russ.) URL: <http://ej.kubagro.ru/2017/06/pdf/07.pdf>
15. Ivanova E.I., Khrustalev E.Yu. [Embedding information technology into public administration and national security issues]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2008, vol. 4, iss. 2, pp. 70–78. URL: <https://cyberleninka.ru/article/v/informatizatsiya-gosudarstvennogo-upravleniya-i-problemy-natsionalnoy-bezopasnosti> (In Russ.)

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.