ОЦЕНКА КАЧЕСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

В.А. Снастин, *магистрант*
Т.П. Харитонов, *магистрант*
Г.Ю. Сорока, *магистрант*
Московский технический университет связи и информатики
(Россия, г. Москва)

DOI:10.24412/2500-1000-2021-8-1-105-108

Аннотация. *В условиях быстрого развития цифровизации необходимо уделять особое внимание обеспечению информационной безопасности. Информационная безопасность тесно связана с обеспечением национальной безопасности страны, поэтому очень важно совершенствовать новейшие информационные технологии с высоким уровнем защиты передачи информации. В статье рассказывается о методах информационной безопасности и информационных системах, используемых в России. В результате, авторы приходят к мнению, что недостаточное обеспечение информационной безопасности – одна из самых приоритетных проблем в Российском сегменте информационных технологий. К тому же высокий рост показателей киберпреступности, говорит о том, что действующие методы по обеспечению информационной безопасности устарели.*

Ключевые слова: *информационные системы, программное обеспечение, киберпреступность, электронная подпись.*

Развитие современных информационных систем в настоящее время имеет огромную скорость. Еще в начале нулевых годов новейшие информационные технологии начали появляться и распространяться среди населения, что дало сильный толчок к формированию информационного общества. Сейчас новейшие технологии присутствуют практически во всех государственных структурах и в жизнедеятельности любого человека. Использование информационных технологий для современного человека является уже чем-то неотъемлемым в жизни.

Современные информационные системы представляют собой комплекс программных продуктов, которые взаимосвязаны и позволяют работать в автономном режиме, это очень удобно, поскольку ускоряет процесс обработки и передачи информации, исключая риски совершения ошибок от человеческого фактора. Для работы и совершенствования таких информационных систем правительство любого государства вкладывает большие деньги т.к. в настоящее время развитие технической сферы любого государства является приоритетной задачей. Чем больше развит технологических сектор государства, тем актуальнее будет продукция данного государства на международных рынках [4].

Несмотря на то, что видимым приоритетом является развитие информационных технологий, на самом деле более важной задачей является обеспечения надежного канала связи для передачи стратегически важной информации. Современные информационные системы обязаны соответствовать всем требованиям надежности и безопасности, исключая риски попадания информации третьим лицам, поэтому обеспечения информационной безопасности является первоочередной задачей для любого государства.

Ядром информационных систем является их программное обеспечение (ПО). Современное программное обеспечение представляет собой сложное многофункциональное изделие, которое обеспечивает работу любой аппаратуры. Исходя из-за сложности создания совершенного программно обеспечения, зачастую в любой программе находиться программные ошибки, непреднамеренные программные дефекты и мало защищенные участки. Именно такими изъянами программы

пользуются злоумышленники для собственных корыстных целей. Главным объектом таких преступлений является утечка информации для возможной дальнейшей ее продажи или же для получения выгоды другими способами. Поэтому программное обеспечение находятся в постоянном совершенствовании и в дополнительной защите от кибератак.

Существует множество способов по обеспечению защиты ПО, а также множество исследований для того, чтобы понимать, как злоумышленник может скрывать вредоносные программы или изменять коды существующих программ для выведения из строя ПО.

Обеспечение информационной безопасности для России играет важную роль, как и для любой другой страны. Во все времена информация является мощнейшим оружием для любой страны. Исходя из этого, обеспечение информационной безопасности в России установлено во многих правовых актов, основой которых является Конституция РФ [1]:

1) ФЗ от 28.12.2010 №390-ФЗ «О безопасности»;

2) ФЗ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»;

3) Закон РФ от 21.06.1993 №5485-1 «О государственной тайне»;

4) ФЗ от 29.07.2004 №98-ФЗ «О коммерческой тайне»;

5) ФЗ от 27.07.2006 №152-ФЗ «О персональных данных»;

6) Уголовный кодекс РФ;

7) Трудовой кодекс РФ;

8) Кодекс РФ об административных правонарушениях;

9) Указ Президента РФ от 17,03.2008 №351 «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена» и т.д.

Все вышеуказанные законодательные меры необходимы для обеспечения информационной безопасности страны. Законодательные акты постоянно совершенствуются, поскольку распространение и возникновение новейших угроз информационной безопасности с каждым годом становится все быстрее. С угрозами киберпространства становится все сложнее бороться из-за оригинальности современных киберпреступников.

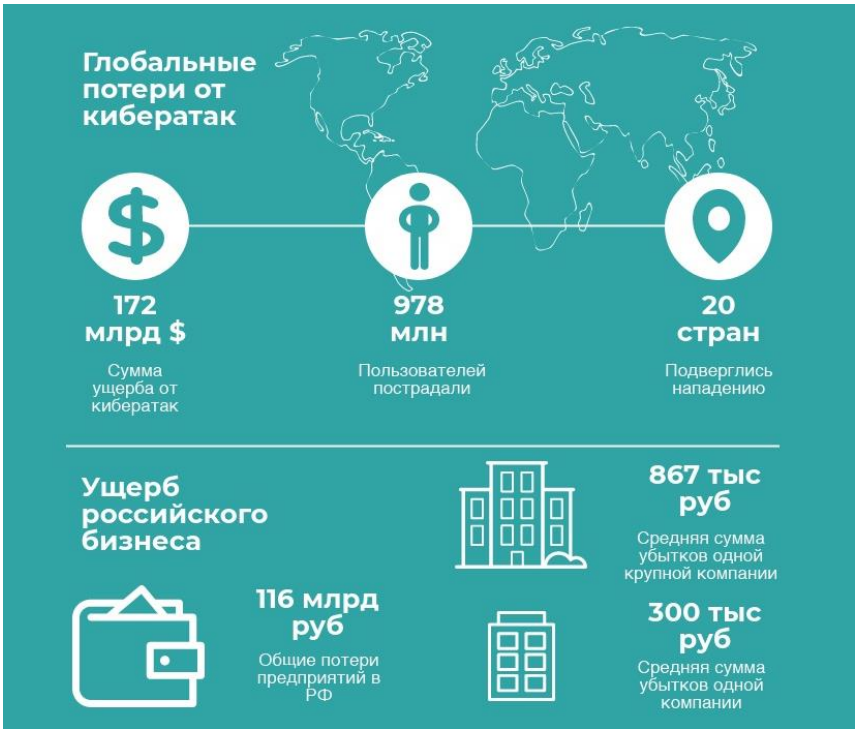

Рис. 1. Ущерб от киберпреступлений: мир и Россия [7]

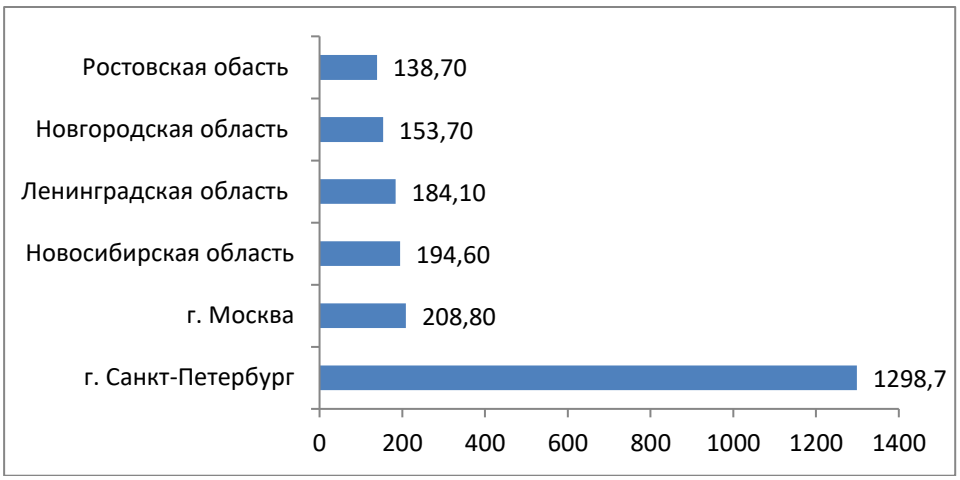

Рис. 2. Регионы с наибольшими темпами прироста зарегистрированных преступлений с использованием информационно-телекоммуникационных технологий, в % [6]

Исходя из вышеуказанных данных, можно сказать, что преступность в сфере информационных технологий несет за собой угрозу экономической безопасности страны. Для обеспечения информационной безопасности страны в государственной программе «Цифровая экономика России» [2] были предусмотрены направления развития, которые обеспечивают более сильную защиту данных.

В основу развития информационных технологий легли приоритетные задачи об обеспечении информационной безопасности. В настоящее время для достижения таких целей идет разработка «облачных» технологий, которые позволят собирать, обрабатывать и анализировать огромный объем информации, находящиеся на различных защищенных серверах. Такие технологии предотвратят заражение персональных компьютеров и другого оборудования вредоносными программами и минимизируют риски по утечки информации.

Также особое внимание уделяется на создание программно обеспечения с несколькими уровнями защиты, которые позволят обнаружить угрозу атаки, при этом давая время для специалистов полностью защитить ПО от злоумышленников.

Поскольку на данный момент Российская Федерация практически полностью перешла на безбумажный документооборот, важной задачей для государства стало обеспечение информационной безопасности на уровне важной документации. Для этого была создана и на данный момент активно используется электронная подпись, которая снижает риски подтелки документов [5].

Исходя из основных задач, которые представлены в проекте «Информационная безопасность», рассчитанная на срок 01.11.2018-31.12.2024 [3], департамент информационной безопасности делает упор на обеспечение безопасности в сети Интернет, а также при совершении платежных операций. Помимо развития «облачных» технологий, также планируется создание защищенных программно-аппаратных комплексов, реализующих технологию распознавание образцов, для использования на беспилотных транспортных средствах. Также программа «Информационная безопасность» подразумевает под собой взятие под полный контроль российский сегмент сети Интернет, что позволит контролировать российское информационное поле и обеспечить достойную защиту информационной безопасности.

Таким образом, можно сделать вывод, что проблема информационной безопасности в России является приоритетной задачей для решения. Важно обеспечивать информационную защиту стратегически важных документов и сведений, которые непосредственно влияют на национальную безопасность страны. Но несмотря на множество проектов, созданных для обеспечения информационной безопасности страны, число киберпреступлений с каждым годом растет. Только в первом полу-

годии 2020 года число киберпреступлений выросло в два раза, в отличие от предыдущего года, и на данный момент киберпреступность составляет 19,9% от общего числа преступлений. Такие данные являются не самыми положительными и правительству РФ требуется уделить большое внимание на методы обеспечения информационной безопасности.

Библиографический список

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). – [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (Дата обращения: 21.10.2020).

2. Распоряжение Правительства РФ от 28.07.2017 программа «Цифровая экономика РФ». – [Электронный ресурс]. – URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (Дата обращения: 22.10.2020).

3. Федеральный проект «Информационная безопасность». – [Электронный ресурс]. – URL: https://digital.gov.ru/uploaded/files/pasport-federalnogo-proekta-informatsionnaya-bezopasnost.pdf (Дата обращения: 23.10.2020).

4. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учеб. пособие для СПО / О.В. Казарин, И.Б. Шубинский. – М.: Изд-во Юрайт, 2019. – 342 с.

5. Маринкин Д.Н. Риски экономических преступлений: информационная безопасность электронной подписи в России // Теоретические и прикладные аспекты противодействия преступности органами внутренних дел. – 2019. – С. 61-65.

6. МВД РФ ФКУ «Главный информативно-аналитический центр» Состояние преступности в России за январь-июль 2020 г. – [Электронный ресурс]. – URL: https://мвд.рф/news/item/20895622 (Дата обращения: 21.10.2020).

7. «Хайтэк» Российский системный интегратор. Инфографика: ущерб от киберпреступлений в 2017. – [Электронный ресурс]. – URL: https://hi-tech.org/press/blog/uscherb-ot-kiberprestuplenii-v-2017 (Дата обращения: 21.10.2020).

ASSESSMENT OF THE QUALITY OF INFORMATION SECURITY IN RUSSIA IN THE CONTEXT OF DIGITALIZATION OF THE ECONOMY

V.A. Snastin, *Graduate Student*
T.P. Kharitonov, *Graduate Student*
G.Yu. Soroka, *Graduate Student*
Moscow Technical University of Communications and Informatics
(Russia, Moscow)

Abstract. *Given the rapid development of digitalization, it is necessary to pay special attention to ensuring information security. Information security is closely linked to ensuring the national security of the country, so it is very important to improve the latest information technologies with a high level of protection of information transmission. The article describes the methods of information security and information systems used in Russia. As a result, the authors come to the conclusion that insufficient information security is one of the highest priority problems in Russian IT segment. In addition, the high growth of cybercrime indicators indicates that the current methods for ensuring information security are outdated.*

Keywords: *information systems, software, cybercrime, electronic signature.*