PREDICTION AND DETECTION METHODS INFORMATION THREATS

Belozerov O.I.[1], Purdikov A.S.[2] (Russian Federation)
Email: Belozerov520@scientifictext.ru

[1]Belozerov Oleg Ivanovich - PhD in Technics, Associate Professor,
DEPARTMENT OF COMPUTER ENGINEERING AND COMPUTER GRAPHICS,
NATURAL SCIENCE INSTITUTE
FAR EASTERN STATE TRANSPORT UNIVERSITY;
[2]Purdikov Andrey Sergeevich – Student,
FACULTY OF LAW,
FAR EASTERN INSTITUTE - BRANCH
ALL-RUSSIAN STATE UNIVERSITY OF JUSTICE (RPA OF THE MINISTRY OF JUSTICE OF RUSSIA),
KHABAROVSK

Abstract: *the article discusses issues related to the content of methods for predicting information threats and the possibility of the emergence of new methods of detecting information threats on the Internet. An analysis of the measures taken, the requirements of the Information Security Doctrine is made. Specific examples of specialized software for compliance with the required security measures are given. Separate information security problems that may arise during the transmission of information in computer networks are highlighted and classified: interception of information, modification of information and substitution of authorship of information.*
Keywords: *information security, software implementation of information protection methods, information security of data transmission, information security.*

МЕТОДЫ ПРОГНОЗИРОВАНИЯ И ОБНАРУЖЕНИЯ ИНФОРМАЦИОННЫХ УГРОЗ

Белозеров О.И.[1], Пурдиков А.С.[2] (Российская Федерация)

[1]Белозеров Олег Иванович - кандидат технических наук, доцент,
кафедра вычислительной техники и компьютерной графики,
Естественно-научный институт
Дальневосточный государственный университет путей сообщения;
[2]Пурдиков Андрей Сергеевич — студент,
юридический факультет,
Дальневосточный институт - филиал
Всероссийский государственный университет юстиции (РПА Минюста России),

г. Хабаровск

Аннотация: *в статье рассматриваются вопросы, связанные с содержанием методов прогнозирования информационных угроз и возможности появления новых способов обнаружения информационных угроз в сети Интернет. Сделан анализ принимаемых мер, требований Доктрины информационной безопасности. Приведены конкретные примеры специализированного программного обеспечения для соблюдения требуемых мер безопасности. Выделены и классифицированы отдельные проблемы информационной безопасности, которые могут возникать при передаче информации в компьютерных сетях: перехват информации, модификация информации и подмена авторства информации.*
Ключевые слова: *информационная безопасность, программная реализация методов защиты информации, информационная безопасность передачи данных, обеспечение безопасности информации.*

XX век подарил миру немало новых технических и научных открытий значительно облегчивших жизнь человека. С появлением сети интернет, например, стало намного проще находить нужную для нас информацию. Но не все источники необходимой нам информации являются безопасными. Пользователи сети всё чаще и чаще становятся жертвами злоумышленников, которые пытаются либо завладеть чужой информацией, либо фальсифицировать информацию для получения той или иной выгоды. Государство предпринимает ряд мер по прогнозированию и обнаружению таких злоумышленников и возможных информационных угроз: как с внутренней, так и с внешней стороны.

Как отмечается в доктрине информационной безопасности Российской Федерации [1], обеспечение информационной безопасности достигается путём осуществления взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, научно-технических, информационно-аналитических, экономических, и иных мер по прогнозированию, сдерживанию, предотвращению информационных угроз и ликвидации последствий после их проявлений.

Для обнаружения попыток несанкционированного доступа к информации, как правило, проводится постоянное исследование журналов с помощью ArcSight Logger и иных подобных программ. Используется системы видеонаблюдения и контроля управления доступом. Осуществляется защита от компьютерных вирусов с помощью использования антивирусных программ и ограничение доступа в помещения, в которых происходит обработка информации. Доступ к обработке и передаче конфиденциальной информации разрешен только для проверенных лиц, обладающих соответствующими допусками. Хорошие результаты дает использование криптографических кодов при

передаче ценной информации - программа “КриптоПро” позволяет контролировать доступ к операциям шифрования и криптографическим ключам, она использует криптографические алгоритмы, разработанные и рекомендованные ФСБ России. Для исследования защищённости применяется так же программная система XSpider Professional Edition и сетевой сканер XSpider.

Для реализации подсистемы обнаружения вторжений используется комплекс StoneGate FireWall. С его помощью производится обнаружение и предотвращение попыток вторжения в режиме реального времени, защита от атак, влекущих за собой подмену адресов, блокировку или завершение запрещённых сетевых соединений [2].

На сегодняшний день, мы можем выделить некоторые проблемы информационной безопасности, которые могут возникать при передаче информации в компьютерных сетях, такие проблемы можно разделить на три основных типа: перехват информации, модификация информации и подмена авторства информации. И каждая из этих проблем может повлечь за собой очень серьёзные последствия. К примеру, злоумышленник может совершить перехват вашего отправленного письма и отослать его от вашего имени. Либо Web-сервер может выдать себя за интернет-магазин и принимать ваши заказы, номера кредитных карт, но, по итогу, никаких товаров не выслать. И для того, чтобы пользователь не попадал на такие “интернет-магазины”, многие антивирусные программы, обнаруживая подобные вредоносные сайты, оповещают пользователя либо блокируют доступ к ним, защищая тем самым его персональные данные.

Информационным угрозам также могут быть подвержены атомные электростанции, химические предприятия, медицинские клиники и т.д. Как показывает практика, более 90% всех проблем в сфере безопасности на таких предприятиях происходят по вине внутренних нарушителей, пытающихся похитить важную информацию. Обеспечение безопасности информации в таких местах достигается комплексом организационных, технических и программных мер. К таким мерам защиты информации относится, например, выявление атак. Качественно реализованные методы защиты информации и обнаружения информационных угроз позволяют обеспечить безопасность информации в полной мере.

Важнейшей составляющей комплексной системы защиты является использование программно-аппаратных средств. Данные средства позволяют реализовать ряд мер, обеспечивающих конфиденциальность информации: идентификацию, аутентификацию, авторизацию, шифрование, контроль целостности, противодействие несанкционированному доступу, противодействие вредоносному программному обеспечению и т.д. Существует также потребность в изобретении и совершенствовании новых методов прогнозирования и обнаружения информационных угроз [3].

Данные вопросы актуальны и для обеспечения информационной безопасности вооруженных сил Российской Федерации. Ведь на смену одним войнам, предусматривающим прямые военные столкновения, приходят войны иного характера, имеющие своей основной целью развитие информационного хаоса на территории противника. И для этого используются все возможности: от хакерских атак на важнейшие системы жизнеобеспечения государства до организации целенаправленной работы средств массовой информации в нужном направлении. Для обеспечения защиты государства вооруженные силы, и их личный состав, проводят ряд мер, связанных с обнаружением и защитой от информационных угроз. К таким методам относятся:

1. Использование DLP-систем, которые реагируют на несоблюдение правил безопасности и правил использования конфиденциальной информации.
2. Методы развития средств электронной разведки.
3. Защита систем от удалённых проникновений в них противника, в частности, с использованием программных ресурсов, обеспечивающих полную защиту периметра от проникновений (например, SIEM-система).
4. Использование социальных сетей для намеренного дезинформационного воздействия на противника.
5. Защита личного состава вооруженных сил от намеренного психологического воздействия противника.

Для реализации данных комплексных мер создаются отдельные подразделения, которые действуют в области информационной безопасности [4].

Необходимо постоянное развитие методов прогнозирования и обнаружения информационных угроз для того, чтобы обеспечить информационную безопасность в полном объеме: как обычных пользователей, так и военных, медицинских и иных организаций.

Список литературы / References

1. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ, 2016. № 50. Ст. 7074.
2. Современные средства связи: материалы XXIII Междунар. науч.-техн. конф., 18–19 окт. 2018 года, Минск, Респ. Беларусь; редкол.: А.О. Зеневич. Минск: Белорусская государственная академия связи, 2018. 304 с.
3. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ, 2016. № 1. Ст. 212.
4. Информационная безопасность вооруженных сил // «SEARCHINFORM». [Электронный ресурс]. Режим доступа:

https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-vooruzhennykh-sil-rf/ (дата обращения: 09.12.2019).