УДК 004

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Романова П.А., студентка 2 курса экономического факультета
Научный руководитель – Бунина Н.Э.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *Интернет, информационная система, сеть, информация, программа, защита.*

В данной статье рассмотрены проблемы защиты информации в системе Интернет. Отмечено, что характер правовых отношений в сети Интернет на данный период времени имеет неблагоприятный характер.

В самой большой сети в мире, Интернете, развертываются атаки на компьютерные системы. Идет постоянная битва интеллектов, организация системных администраторов и изобретательность хакеров.

Проанализируем некоторые методы и средства защиты информации.

Контроль доступа – методы защиты информации путем регулирования использования каждого IP-адреса (IP-адрес имеет доменную структуру и может быть представлен в символьном или цифровом виде [1]).

Контроль доступа включает следующие функции безопасности:

1. идентификация пользователей, персонала и ресурсов системы (привязка к каждому объекту с помощью персонального идентификатора);

2. идентификация (аутентификация) объекта или субъекта в представленном виде идентификатора;

3. проверка учетных данных (проверка соблюдения дня, недели, времени; запрашиваются ресурсы и процедуры в соответствии с установленными правилами);

4. разрешение и создание условий труда в пределах установленных норм;

5. запись обращений к защищаемым ресурсам;

6. реагирование (сигнализация, отключение, задержка работы, отказ в запросе и т. д.) при попытке несанкционированных действий [2].

Все эти методы защиты наиболее широко используются при обработке и хранении информации на магнитных носителях.

Механизм шифрования – криптографическое закрытие информации. При передаче информации по каналам связи на большие расстояния этот метод является единственно надежным.

Борьба с атаками вредоносных программ предполагает различные меры организационного характера и использования антивирусных программ. Цели принятых мер – это снижение вероятности заражения всевозможными вирусными программами и выявление фактов заражения системы; снижение последствий заражения информации, локализации или уничтожения вирусов; восстановление информации в информационной системе [3].

Регулирование – создание таких условий для автоматизированной обработки, хранения и передачи защищенной информации, в которой нормы и стандарты защиты выполняются в наибольшей степени.

Принуждение – это метод защиты, при котором пользователи и персонал интеллектуальной собственности вынуждены соблюдать правила обработки, передачи и использования защищенной информации, подверженной риску материальной, административной или уголовной ответственности.

Побуждение – метод защиты, заставляющий пользователей и сотрудников ИС оставаться в неприкосновенности установленных процедур в связи с соблюдением установленных морально-этических норм. Весь комплекс технических мероприятий делится на аппаратные и физические.

Аппаратное обеспечение – устройства, встроенные непосредственно в вычислительную технику, или устройства, подключающиеся через стандартный интерфейс [4].

К физическим средствам относятся различные инженерные устройства и сооружения, предотвращающие физическое проникновение злоумышленников в защитные объекты и защищающие персонал (средства индивидуальной защиты), материалы и финансы. Примеры физических средств: замки двери, оконные решетки, электронные охранные сигнализации и т. д.

Программные средства – это специальные программы и программные комплексы, разработанные для защиты IP-информации [5,6]. Как уже говорилось, многие из них объединены с программным обеспечением.

Из программных средств системы безопасности необходимо выделить больше программных средств, реализующих механизмы шифрования (криптографии). Криптография – это наука, гарантирующая секретность или подлинность переданных сообщений.

Организационные средства осуществляют комплексное регулирование производства, деятельность в области интеллектуальной собственности и отношения между исполнителями на нормативной основе. Комплекс мероприятий реализуется группой информационной безопасности, которая должна быть под контролем первого проводника.

Средства правовой защиты определяются законодательством страны, в котором правила использования, обработки и передачи информации предоставляются с ограниченным доступом. Получить его можно путем установления меры ответственности за нарушение установленных правил.

Морально-этические средства защиты включают в себя все виды норм поведения, которые традиционно формируются с распространением IP-адресов в стране и в мире или специально разработанные. Моральные и этические стандарты могут быть неписаными (например, честность) или оформленными в виде свода (устава) правил или положений. Эти нормы, как правило, юридически не утверждены, но поскольку несоблюдение их приводит к падению престижа организации, считаются обязательными. Характерным примером таких требований является Кодекс профессионального поведения членов Ассоциации пользователи ЭВМ в Америке.

Таким образом, практика показывает, что во всех странах ущерб от злонамеренных действий носит негативный характер. Кроме того, основные причины потерь в меньшей степени связаны с недостатком средств безопасности как таковой, насколько это связано с отсутствием связи между ними, то есть с нереализованностью системного подхода. Поэтому необходимо как можно быстрее усовершенствовать комплексные средства защиты.

Библиографический список:

1. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер // Рн-Д: Феникс, 2017. – Режим доступа: http://elar.uspu.ru

2. Солнцева, О.В. Современные платформы дистанционного обучения: возможности и недостатки / О.В. Солнцева, Н.Э. Бунина, М.С. Бадашин // Материалы Национальной научно-методической конференции профессорско-преподавательского состава «Инновационные технологии в высшем образовании», 2018. – С. 54–60.

3. Бунина, Н.Э. Риски и преимущества дистанционного образования / Н.Э. Бунина// Материалы Всероссийской научно-практической конференции «Современные тенденции развития системы образования». – Чебоксары, 2020. – С. 55–58.

4. Бунина, Н.Э. Тенденции развития цифровой экономики / Н.Э. Бунина, О.А. Заживнова, А.В. Коновалов // Материалы Национальной научно-практической конференции «Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения». – Ульяновск, 2019. – С. 238–242.

5. Бунина, Н.Э. Интерактивное взаимодействие как основа курса дистанционного обучения/ Н.Э. Бунина // Материалы Всероссийской научно-практической конференции «Образование и педагогика, теория и практика». – Чебоксары, 2020. – С. 290–293.

6. Солнцева, О.В. Анализ статистических данных в пакете Statistica 5.5 / О.В. Солнцева, А.В. Севастьянов.- Ульяновск, 2004. Часть I

INFORMATION SECURITY SYSTEM ON THE INTERNET

Romanova P.A.

Key words: *Internet, information system, network, information, program, protection.*

This article discusses the problems of information security in the Internet system. It is noted that the nature of legal relations on the Internet for this period of time is unfavorable.