отметить, что немаловажным фактором в оценке дистанционного формата обучения является отношение к нему участников образовательного процесса. Мнения противоречивы: одни считают сочетание онлайн и оффлайн обучения лучшим, если не единственным, вариантом в сложившихся условиях, полагая, что у этого формата есть будущее; другие не очень положительно относятся к внедряемым новшествам.

Так, мы видим, что соотношение плюсов и минусов данного формата каждый определяет для себя сам. Несомненно, подавляющая часть участников дистанционного обучения, овладела достаточным количеством навыков работы с продуктами передовой технологии, что является безусловным плюсом. В то же время определенный пласт материала не был освоен в связи с техническими неполадками в процессе обучения и зачастую недостаточной самодисциплинированностью учащихся, что, однако, является весомым недостатком.

Таким образом, ясно видно, что система образования претерпевает существенные, а то и неотвратимые изменения, преподнося людям все новые и новые вопросы, на которые им необходимо найти ответы. Однако поиск этих ответов займёт определенный период времени, до истечения которого нам остаётся лишь предполагать, анализировать, делать прогнозы и давать те или иные оценки.

1. Понятие дистанционного обучения <http://informatizaciya.forum2x2.ru/t33-topic>
2. Дистанционное образование: плюсы и минусы <http://dtraining.web3.ru/introduction/okandbaddo/>
3. Концепция внедрения систем электронного дистанционного обучения в деятельность образовательных учреждений Российской Федерации <http://www.openclass.ru/node/289858>

Белоглазов К.В., Мальков К.Н., Ермолаева В.В.

Защита информации в жизни людей

*ФГБОУ ВО «Саратовский государственный технический университет имени
Гагарина Ю.А.»
(Россия, Саратов)*

doi: 10.18411/lj-12-2020-03

idsp: ljjournal-12-2020-03

Аннотация

В данной статье рассматривается защита информации, как отдельная сфера информационных технологий, её роль в современном мире, способы защиты информации. Рассмотрена система защиты, используемая в Российской Федерации и доктрина, определяющая направление развития информационной безопасности в РФ.

Ключевые слова: информационная безопасность, защита информации, средства защиты, программное обеспечение.

Abstract

This article discusses information security as a separate area of information technology, its role in the modern world, and ways to protect information. The article considers the security system used in the Russian Federation and the doctrine that determines the direction of information security development in the Russian Federation.

Keywords: information security, security tools, software.

Понятия информационной безопасности (ИБ) являются базовыми, так как их сущность определяет как деятельность в среде защиты информации, так и политику. В то же время эти понятия сильно взаимосвязаны в этой сфере.

Информационная защита – это организационные, правовые, технические и технологические меры по предупреждению угроз информационной безопасности и устранению их последствий.[4]

В наше время можно утверждать, что с каждым днем появляются новшества, и развитие информационной безопасности не осталось без внимания. Для реализации этой технологии требуются высокоценные специалисты, которые знают свое дело, также эта сфера полна расходов и усилий. Несомненно, ИБ является безумно сложным процессом, однако все это позволяет избежать возможного ущерба от злоумышленников.

Вирусы – это опасные программы, суть которых - повредить файлы или программное обеспечение.

Антивирусная программа – важная составляющая каждой компьютерной машины, предназначенная для поиска и устранения вредоносного программного обеспечения.

Существует вирус под названием «Троянский конь». Он является опасной программой, которая выглядит на первый взгляд безопасной, например компьютерными играми, но после активации может повредить файлы, при этом пользователь даже не будет уведомлен об этом.

Исходя из этого, каждому человеку необходимо защищать себя от заражения вирусным ПО. По статистике, вирусы могут наносить ущерб до нескольких десятков миллионов долларов в год. Но чего придерживаются создатели антивирусов при их создании?

Для защиты информации требуется не узконаправленный, а комплексный подход к созданию механизмов защиты. Для обеспечения качественной защиты, включая все условности и тонкости, необходимо следовать принципам:

- Соответствие уровня защиты степени ценности информации;
- Гибкость защиты;
- Многозональность средств защиты (т.е. размещение источников информации в зонах с контролируемым уровнем её безопасности);
- Многорубежность средств защиты информации на пути движения вражеского агента (или технического средства разведки).
- Соответствие уровня защиты ценности информации. Этот принцип определяет экономическую целесообразность тех или иных мер защиты.[1]

Но, даже если соблюдать эти принципы, нет гарантий на сохранность информации. Какой бы совершенной не была система защиты, её необходимо регулировать действиями человека.

Рассмотрим основные методы обеспечения информационной безопасности. Во-первых, это охрана источников информации. Не доходя до создания защитного ПО, люди должны создать физически защищённые сервера с базами данных. Злоумышленник не должен иметь к ним доступ. То есть такие места должны быть охраняемым объектом с ограниченным доступом. Во-вторых, это программная маскировка.

Программная маскировка обеспечивается преобразованием информационного портрета. Информационный портрет – это объединение элементов и частей между ними, отображающих смысл сообщения и свойства объекта. Существуют способы изменения информационного портрета:

- Удаление части элементов и свойств, образующих информационный узел;
- Преобразование части элементов информационного портрета при сохранении стабильности связей между оставшимися элементами;
- Удаление или изменение свойств между элементами информационного портрета при поддержке их общего числа.

Одним из важных средств обеспечения ИБ персональных данных в Российской Федерации является Dallas Lock 8. Его сущность – совокупность средств защиты информации, как в технических, так и в информационных системах, обрабатывающих

персональные данные. В состав СЗИ Dallas Lock 8.0 включена подсистема очистки остаточной информации, гарантирующая отсутствие возможности восстановления ранее удалённых данных. Это происходит во время освобождения областей на дисках и очистки файла подкачки Windows. Также данная подсистема гарантирует очистку используемого пространства оперативной памяти. В Dallas Lock существует команда форматирования при подключении любого незарегистрированного пользователя.[2]

Текущее положение *информационной безопасности в нашей стране* – это состояние новой, только появившейся и развивающейся сферы информационных технологий. Основой для дальнейшего решения проблем и развития данной сферы стало утверждение Президентом РФ в сентябре 2001г. *Доктрины информационной безопасности Российской Федерации*.

В Доктрине рассматриваются:

- Причины угроз ИБ;
- Последствия возможных угроз ИБ;
- Методы устранения угроз ИБ;
- Обеспечение ИБ в жизнедеятельности общества;
- Основные положения государственной политики по обеспечению ИБ.

Важная задача состоит в учёте интересов государства и граждан Доктрина. Эти интересы определяет следующим образом:

- Интересы личности в информационной сфере устанавливаются в осуществлении конституционных прав человека на доступ к информации;
- Интересы общества в информационной сфере устанавливаются в обеспечении интересов общества в этой области и создании правового социального государства;
- Интересы государства в информационной сфере устанавливаются в образовании лучших условий для развития российской информационной инфраструктуры, осуществления конституционных прав и свобод человека в области получения информации;
- Следование принципа баланса интересов граждан, общества и государства в информационной сфере располагает законодательное фиксирование приоритета этих интересов в различных областях жизнедеятельности общества, а также применение различных форм общественного контроля над работой федеральных органов государственной власти и органов государственной власти субъектов РФ.[3]

Опираясь на понятие защиты информации, можно сделать следующие выводы: защита информации – совершенствующаяся сфера информационных технологий, так как развитие вирусного ПО не стоит на месте; организация безопасности не равномерна, а ступенчатая. Основные методы защиты информации делятся на два типа: физические и программные. Физические не позволяют добраться до территории, на которой находится защищённая информация, а программные не позволяют получить эту информацию удалённым способом через компьютер.

1. Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Гайнулин Т.Р. Методы и средства инженерно-технической защиты информации: учебное пособие 2012. 187 с.
2. Прокушева А.П., Возможности СЗИ от НСД Dallas lock 8 для обеспечения информационной безопасности персональных данных. Прокушева А.П., Прокушев Я.Е., Пономаренко С.В. Успехи современной науки и образования. 2017. 166-169 с.
3. С.В.Петров, П.В.Петров., Информационная безопасность человека и общества: учебное пособие. 2007. 336 с
4. <https://cyberleninka.ru/article/n/sovremennyye-sposoby-zaschity-informatsii-i-informatsionnaya-bezopasnost>