

УДК 378.14

**Коляда А.С.**, аспірант,  
**Гогунский В.Д.**, д.т.н., проф.,  
*кафедра управління системами безпеки  
жизнедеятельности*

---

## ПРЕДОТВРАЩЕНИЕ ИНФОРМАЦИОННОЙ ОПАСНОСТИ

---

*А. С. Коляда, В. Д. Гогунский. Предотвращение информационной опасности. Рассматривается организационный уровень защиты данных, наиболее распространённые ошибки пользователей и рекомендации по обеспечению достаточного уровня безопасности данных следуя простым правилам.*

**Ключевые слова:** защита данных, пароли, безопасность, правила.

*A. S. Kolyada, V. D. Gogunsky. Prevention of information risk. We consider the organizational level of data protection, the most common user errors and recommendations to ensure a sufficient level of data security by following the simple rules.*

**Ключові слова:** захист даних, паролі, безпека, правила.

*А. С. Коляда, В. Д. Гогунський. Запобігання інформаційної небезпеки. Розглядається організаційний рівень захисту даних, найбільш поширені помилки користувачів і рекомендації щодо забезпечення достатнього рівня безпеки даних слідуючи простим правилам.*

**Keywords:** data protection, passwords, security, rule.

Информационная безопасность является практикой защиты информации от несанкционированного доступа, использования и раскрытия информации, нарушению, модификации, чтения, проверки, записи или уничтожения. Это общий термин, который может быть использован независимо от формы данных (электронной, физической, и т.д.) [1]

В настоящее время большая часть информации собирается, обрабатывается и хранится на электронных вычислительных машинах и передается по сети на другие компьютеры. Поэтому область информационной безопасности выросла и развилась значительно в последние годы.

Конфиденциальность, целостность и доступность данных являются основными принципами информационной безопасности [2]. Точками приложения процесса защиты информации к информационной системе являются аппаратное обеспечение, программное обеспечение и коммуникации. Сами процедуры (механизмы) защиты разделяются на защиту физического уровня, защиту персонала и организационный уровень (рис. 1). Данная статья рассматривает организационный или административный уровень защиты.

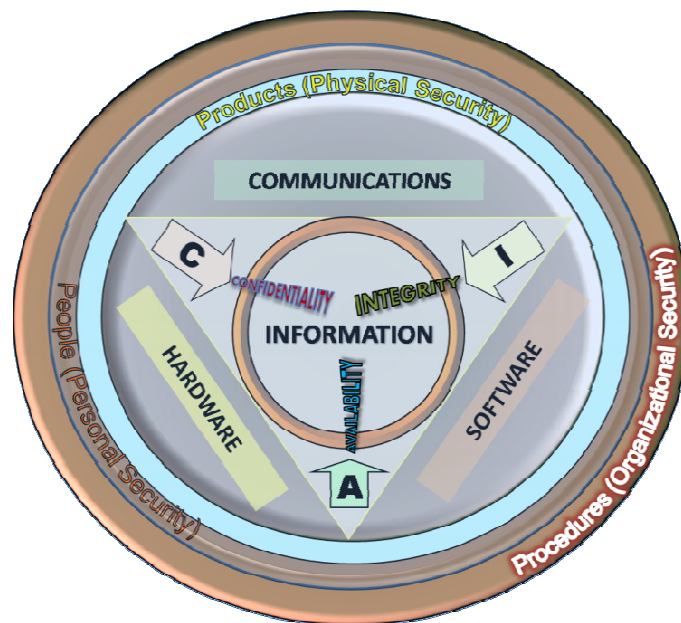


Рис. 1. Компоненты информационной безопасности

Административный контроль состоит из процедур, стандартов и политик которые информируют людей о том, как пользоваться продуктом и какие операции проводить для обеспечения информационной безопасности в организациях. Государственные законы и правила являются примером административного контроля. Другими примерами являются политика паролей, политика набора персонала, дисциплинарная политика.

Административный контроль имеет первостепенное значение и является основой для физического и логического уровня защиты информации.

Главный вопрос состоит в том, как предотвратить возможность несанкционированного доступа к информации.

Согласно исследованиям специалистов из Symantec (компания по производству программного обеспечения в области информационно безопасности) есть много простых ошибок в действиях пользователей, которые значительно понижают уровень безопасности компьютера. Ниже перечислены 5 основных ошибок [3]:

1. Приложения и операционные системы не обновляются регулярно;
2. Иметь открытый доступ к компьютеру, как из сети, так и физически;
3. Не соблюдения политики паролей – использование стандартных или легко узнаваемых паролей;
4. Небезопасное хранение данных – использование открытых хранилищ и неконтролируемый доступ к данным.
5. Нет обучения пользователей поведению в социальных сетях и различных онлайн приложениях.

Несоблюдение простых правил может привести к плачевным результатам.

Примером такого результата может служить статья [4], где рассказано как, зная только имя и адрес электронной почты человека, злоумышленники получили доступ ко всем его аккаунтам и удаленно уничтожили информацию на всех его устройствах.



критериям безопасного пароля, то на каждом сайте должен использоваться уникальный пароль, но человеку трудно запомнить всех их, поэтому большинство использует одинаковые пароли.

Для облегчения ситуации, можно использовать один, но надежный пароль (мастер пароль). С помощью его можно защитить хранилище всех остальных паролей. Существуют специализированные программы – менеджеры паролей, которые помогают вам сгенерировать достаточно надежные пароли, которые вам запоминать не нужно, а достаточно помнить один – для входа в менеджер. Примерами таких программ являются KeyPass (<http://keepass.info/>), LastPass (<https://lastpass.com/>).

Таким образом, главное в информационной безопасности, как и в безопасности в целом, является предотвращение опасности [7 ... 12]. Следуя простым правилам и не пренебрегая базовым политикам безопасности можно поддерживать достаточный уровень безопасности данных. Необходимо поддерживать программное обеспечение в актуальном состоянии, контролировать доступ к данным, использовать надежные пароли и не открывать / запускать неизвестные приложения. Следуя этим правилам можно обезопасить себя от значительного количества угроз.

#### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. [http://en.wikipedia.org/wiki/Information\\_security](http://en.wikipedia.org/wiki/Information_security) [Электронный ресурс].
2. <http://www.techrepublic.com/blog/security/the-cia-triad/488> - [Электронный ресурс].
3. <http://dailyinfographic.com/top-5-computer-security-mistakes-infographic> - [Электронный ресурс]
4. <http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/> - [Электронный ресурс].
5. <http://habrahabr.ru/post/178195/> - [Электронный ресурс].
6. Mark Burnett, Perfect Password: Selection, Protection, Authentication. Syngress, 2005. – 182 p. ISBN-10: 1597490415, ISBN-13: 978-1597490412.
7. Михайловский, С.Л. Автоматизированная подсистема конвертирования символов различных операционных систем [Текст] / С. Л. Михайловский, В. Д. Гогунский // Труды ученых Одес. политехн. ун-та. - Вып. 2 (8). – Одесса : ОГПУ, 1999. — С 104 – 107.
8. Тертышная, Т. И. Автоматизированная система контроля знаний [Текст] / Т. И. Тертышная, Е. В. Колесникова, В. Д. Гогунский // Труды Одес. политехн. ун-та. — Вып. 1 (13). — Одесса : ОГПУ, 2001. — С. 125 – 128.
9. Яковенко, В. Д. Формалізація вимог до системи автоматизованого управління навчальним закладом [Текст] / В. Д. Яковенко, В. Д. Гогунський, О. В. Нарожний // Моделир. в прикл. науч. исследованиях. Матер. XVI семинара. — Одесса : ОНПУ, 2008. – С. 9 – 12.
10. Оборський, Г.О. Стандартизація і сертифікація процесів управління якістю освіти у вищому навчальному закладі [Текст] / Г. О. Оборський, В. Д. Гогунський, О. С. Савельєва // Труды Одес. политехн. ун-та. – Вып. 1(35). – Одесса : ОНПУ, 2011. – С. 251 – 255.
11. Колесніков, О. Є. Основні аспекти впровадження дистанційної освіти [Текст] / О. Є. Колесніков, В. Д. Гогунський // Інформаційні технології в освіті, науці та виробництві. – Вип. 1(1). – Херсон : АО Бахва, 2012. – С. 34 – 41.

12. Яковенко, А.Е. Стратегия принятия решений в условиях адаптивного обучения [Текст] / А.Е. Яковенко А.В. Нарожный, В.Д.Гогунский // Восточно-европейский журнал передових технологий. – 2/2(14). – 2005. – С.105 – 110.