Столыпинский
вестник

Научная статья
Original article
УДК 004.424

ЭТИКА И ИНТЕРНЕТ

ETHICS AND THE INTERNET

Крыгин Никита Дмитриевич, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), krigginnn@rambler.ru

Krygin Nikita Dmitrievich, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), krigginnn@rambler.ru

Аннотация: Этика – это вопрос личной неприкосновенности. Профессия системной безопасности заключается в том, чтобы делать то, что правильно, и останавливать то, что неправильно. Использование Интернета является привилегией, разделяемой всеми. Это средство коммуникации без границ, без культурных предубеждений и без предубеждений. Пользователи имеют право на подключение. Это то, за что нужно быть благодарным. К сожалению, плохие парни используют киберпространство для совершения преступлений и создания проблем. Это создало глобальную потребность в специалистах по безопасности систем.

Abstract: Ethics is a matter of personal integrity. The profession of system security is about doing what is right and stopping what is wrong. Using the Internet

is a privilege shared by all. It is a means of communication without borders, without cultural bias and without prejudice. Users have the right to connect. This is something to be thankful for. Unfortunately, the bad guys use cyberspace to commit crimes and create problems. This has created a global need for systems security specialists.

Ключевые слова: информационная безопасность, этика, интернет

Keywords: information security, ethics, internet

Представьте, если бы не было авиадиспетчеров и самолеты летали бы свободно. Попытка взлететь и приземлиться была бы чрезвычайно опасной. Вероятно, аварий было бы намного больше. Такая ситуация приведет к хаосу.

Невероятно, но в киберпространстве нет властей, функционирующих как авиадиспетчеры. Что еще хуже, человеческое поведение в сети часто менее зрелое, чем в обычных социальных условиях. Киберпространство стало новой площадкой для сегодняшних плохих парней. Вот почему спрос на специалистов по системной безопасности растет так быстро.

Структура политики ИТ-безопасности

Киберпространство не может продолжать процветать без определенных гарантий безопасности пользователей. Несколько законов теперь требуют от организаций хранить личные данные в тайне. Предприятия не могут эффективно в Интернете, где любой может украсть свои данные. ИТ-безопасность имеет решающее значение для выживания любой организации. Этот раздел знакомит вас с основой политики ИТ-безопасности . Структура состоит из политик, стандартов, процедур и руководств, которые снижают риски и угрозы.

Определения

Структура политики безопасности ИТ состоит из четырех основных компонентов:

Политика — Политика — это краткое письменное заявление, которое люди, отвечающие за организацию , установили в качестве курса действий или

направления. Политика исходит от высшего руководства и применяется ко всей организации.

Стандарт — стандарт представляет собой подробное письменное определение аппаратного и программного обеспечения и способов их использования. Стандарты гарантируют, что во всей ИТ-системе используются согласованные меры безопасности.

Процедуры — это письменные инструкции о том, как использовать политики и стандарты. Они могут включать план действий, установку, тестирование и аудит средств управления безопасностью.

Руководящие принципы — руководящие принципы представляют собой предлагаемый курс действий по использованию политики, стандартов или процедур. Рекомендации могут быть конкретными или гибкими в отношении использования.

Политики применяются ко всей организации. Стандарты специфичны для данной политики. Процедуры и рекомендации помогают определить использование. В рамках каждой политики и стандарта определите воздействие для семи доменов типичной ИТ-инфраструктуры. Это поможет определить роли, обязанности и подотчетность во всем.

Основополагающие политики ИТ-безопасности

В центре внимания структуры политики ИТ-безопасности вашей организации является снижение вашей подверженности рискам, угрозам и уязвимостям. Важно связать определение политики и стандарты с практическими требованиями к дизайну. Эти требования будут надлежащим образом применять лучшие меры безопасности и контрмеры. Заявления о политике должны устанавливать ограничения, а также ссылаться на - стандарты, процедуры и руководящие принципы. Политики определяют, как должны использоваться меры безопасности и контрмеры для соблюдения законов и нормативных актов.

Примеры некоторых основных политик ИТ-безопасности включают следующее:

Политика допустимого использования (AUP) — AUP определяет действия, которые разрешены и запрещены в отношении использования ИТ-активов, принадлежащих организации. Эта политика специфична для пользовательского домена и снижает риск между организацией и ее сотрудниками.Политика осведомленности о безопасности — эта политика определяет, как обеспечить осведомленность всего персонала о важности безопасности и поведенческих ожиданиях в соответствии с политикой безопасности организации. Эта политика специфична для пользовательского домена и актуальна, когда вам нужно изменить поведение осведомленности о безопасности организации.

Политика классификации активов — эта политика определяет стандарт классификации данных организации. Он сообщает, какие ИТ-активы имеют решающее значение для миссии организации. Обычно он определяет системы организации, их использование и приоритеты данных, а также идентифицирует активы в семи доменах типичной ИТ-инфраструктуры.

Политика защиты активов — эта политика помогает организациям определить приоритет для критически важных ИТ-систем и данных. Эта политика соответствует анализу воздействия на бизнес (BIA) организации и используется для устранения рисков, которые могут угрожать способности организации продолжать работу после аварии.

Политика управления активами — эта политика включает операции по обеспечению безопасности и управление всеми ИТ-активами в семи доменах типичной ИТ-инфраструктуры.

Оценка уязвимостей и управление ими — эта политика определяет окно уязвимости для всей организации для производственной операционной системы и прикладного программного обеспечения. На основе этой политики вы разрабатываете общеорганизационные стандарты, процедуры и рекомендации по оценке уязвимостей и управлению ими.

Оценка и мониторинг угроз — эта политика определяет полномочия по оценке и мониторингу угроз в масштабах всей организации. Вы также должны

включить в эту политику конкретные сведения о домене LAN-to-WAN и соответствии AUP.

Организациям необходимо адаптировать свою политику ИТ-безопасности к своей среде. После проведения оценки безопасности своей ИТ-системы многие организации согласовывают определения политик с пробелами и уязвимыми местами. Политика обычно требует рассмотрения и одобрения исполнительным руководством и главным юрисконсультом.

Литература

1. Алеексеев, П. Антивирусы. Настраиваем защиту компьютера от вирусов / П. Алеексеев, Д. Козлов, Р. Прокди. - М.: СПб: Наука и Техника, 2018. - 915 с.
2. Александров, К.П. Компьютер без сбоев, вирусов и проблем / К.П. Александров, Р.Г. Прокди. - М.: Наука и техника, 2017. - 192 с.
3. Алямовский, А.А. SolidWorks 2007/2008. Компьютерное моделирование в инженерной практике / А.А. Алямовский. - М.: СПб: БХВ-Петербург, 2017. - 845 с.
4. Большаков, В.П. Инженерная и компьютерная графика. Практикум: моногр. / В.П. Большаков. - М.: СПб: БХВ, 2020. - 592 с.
5. Бухбергер, Б. Компьютерная алгебра: символьные и алгебраические вычисления / Б. Бухбергер, Дж. Коллинз, Р. Лоос. - М.: [не указано], 2020. - 344 с.
6. Вульф, М.М. Защита компьютера от вирусов (книга + видеокурс на DVD) / М.М. Вульф, Н.Т. Разумовский. - М.: СПб: Наука и Техника, 2020. - 160 с.
7. Глушаков, С.В. Компьютерная верстка. QuarkXPress 4.1. Adobe PageMaker 6.52. Учебный курс / С.В. Глушаков, Г.А. Кнабе. - М.: Харьков: Фолио, 2016. - 485 с.
8. Глушаков, С.В. Компьютерная графика / С.В. Глушаков, Г.А. Кнабе. - М.: Харьков: Фолио, 2016. - 500 с.
9. Гурский, Ю. Компьютерная графика: Photoshop CS, CorelDRAW 12,

Illustrator CS / Ю. Гурский, И. Гурская, А. Жвалевский. - М.: СПб: Питер, 2016. - 812 с.

10. Дабижа Компьютерная графика и верстка. CorelDRAW, Photoshop, PageMaker / Дабижа, Галина. - М.: СПб: Питер, 2017. - 272 с.
11. Девянин, П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, 2020. - 176 с.
12. Зарецкий, А.В. А я был в компьютерном городе / А.В. Зарецкий, А.В. Труханов. - М.: Просвещение, 2018. - 208 с.
13. Зенкин, А.А. Когнитивная компьютерная графика / А.А. Зенкин. - М.: Наука, 2018. - 192 с.
14. Касихин, В.В. Как стать создателем компьютерных игр. Краткое руководство / В.В. Касихин. - М.: Вильямс, 2016. - 208 с.
15. Кротов, Н.Н. Nero Burning ROM 8. Компьютерная шпаргалка / Н.Н. Кротов, Р.Г. Прогди. - М.: СПб: Наука и Техника, 2020. - 594 с.
16. Кук, Д. Компьютерная математика / Д. Кук, Г. Бейз. - М.: [не указано], 2020. - 431 с.

References

1. Alekseev, P. Antiviruses. Setting up computer protection against viruses / P. Alekseev, D. Kozlov, R. Prokdi. - M.: St. Petersburg: Science and Technology, 2018. - 915 p.
2. Alexandrov, K.P. Computer without failures, viruses and problems / K.P. Aleksandrov, R.G. Prokdi. - M.: Science and technology, 2017. - 192 p.
3. Alyamovsky, A.A. SolidWorks 2007/2008. Computer modeling in engineering practice / A.A. Alyamovsky. - M.: St. Petersburg: BHV-Petersburg, 2017. - 845 p.
4. Bolshakov, V.P. Engineering and computer graphics. Workshop: monograph. / V.P. Bolshakov. - M.: St. Petersburg: BHV, 2020. - 592 p.
5. Buchberger, B. Computer algebra: symbolic and algebraic calculations / B. Buchberger, J. Collins, R. Loos. - M.: [not specified], 2020. - 344 p.

6. Wolf, M.M. Protecting your computer from viruses (book + video course on DVD) / M.M. Wolf, N.T. Razumovsky. - M.: St. Petersburg: Science and Technology, 2020. - 160 p.
7. Glushakov, S.V. Computer layout. QuarkXPress 4.1. Adobe Page Maker 6.52. Training course / S.V. Glushakov, G.A. Knabe. - M.: Kharkov: Folio, 2016. - 485 p.
8. Glushakov, S.V. Computer graphics / S.V. Glushakov, G.A. Knabe. - M.: Kharkov: Folio, 2016. - 500 p.
9. Gursky, Yu. Computer graphics: Photoshop CS, CorelDRAW 12, Illustrator CS / Yu. Gursky, I. Gurskaya, A. Zhvalevsky. - M.: St. Petersburg: Piter, 2016. - 812 p.
10. Dabija Computer graphics and layout. CorelDRAW, Photoshop, PageMaker / Dabizha, Galina. - M.: St. Petersburg: Piter, 2017. - 272 p.
11. Devyanin, P.N. Security analysis of access control and information flows in computer systems / P.N. Devyanin. - M.: Radio and communication, 2020. - 176 p.
12. Zaretsky, A.V. And I was in a computer city / A.V. Zaretsky, A.V. Trukhanov. - M.: Education, 2018. - 208 p.
13. Zenkin, A.A. Cognitive computer graphics / A.A. Zenkin. - M.: Nauka, 2018. - 192 p.
14. Kasikhin, V.V. How to become a computer game creator. Brief guide / V.V. Kasikhin. - M.: Williams, 2016. - 208 p.
15. Krotov, N.N. Nero Burning ROM 8. Computer cheat sheet / N.N. Krotov, R.G. Progdie. - M.: St. Petersburg: Science and Technology, 2020. - 594 p.
16. Cook, D. Computer Mathematics / D. Cook, G. Baze. - M.: [not specified], 2020. - 431 p.

Для цитирования: Крыгин Н.Д. Этика и интернет Научный сетевой журнал «Столыпинский вестник», номер 4/2022.