Гайнутдинова А.Р., Часов П.С. Основы информационной безопасности и способы защиты информационных технологий // Международный журнал информационных технологий и энергоэффективности. – 2022. –
Т. 7 № 4(26) часть 2 с. 56–61

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

[1] Гайнутдинова А.Р., [2] Часов П.С.

МИРЭА-Российский технологический университет (РТУ МИРЭА)
Институт информационных технологий, Москва, Россия (119454, г. Москва, проспект Вернадского, д. 86, с2), e-mail: [1] ddagaynutdinova@mail.ru, [2] pasha_chasov@mail.ru

В данной статье рассмотрена проблема, связанная с защитой информации, ее определение и общий смысл. Также были определены основные меры обеспечения безопасности и уровни его предоставления.

Ключевые слова: информационные технологии, информационная безопасность, кибератака, вирусы, программное обеспечение, техническое средство, криптографическая защита, обработка данных, хранение данных, передача данных.

FUNDAMENTALS OF INFORMATION SECURITY AND WAYS TO PROTECT INFORMATION TECHNOLOGIES

[1] Gainutdinova A.R., [2] Chasov P. S.

MIREA-Russian Technological University (RTU MIREA), Institute of Information Technology, Moscow, Russia (119454, Moscow, Vernadskogo Avenue, 86, p2), e-mail: [1] ddagaynutdinova@mail.ru, [2] pasha_chasov@mail.ru

This article discusses the problem related to the protection of information, its definition and general meaning. The main security measures and levels of its provision were also identified.

Keywords: information technology, information security, cyberattack, viruses, software, hardware, cryptographic protection, data processing, data storage, data transmission.

В условиях динамического развития электронно-коммуникационных технологий, которые способствуют повышению эффективности и производительности, возникает вопрос о производимой этими же технологиями проблемы с точки зрения безопасности. Хотя новые технология и являются мощными, они также достаточно уязвимы. [1, 2]

Несмотря на то, что информационные технология зарекомендовали себя как надежные устройства в рекомендациях часто просят проявлять осторожность и принимать многочисленные меры предосторожности для повышения безопасности. Вирусы, вторжения, сбои в работе – все это обычные опасности в мире, где общение и обмен потоком знаний и информацией как облегчается, так и подвергается угрозе.

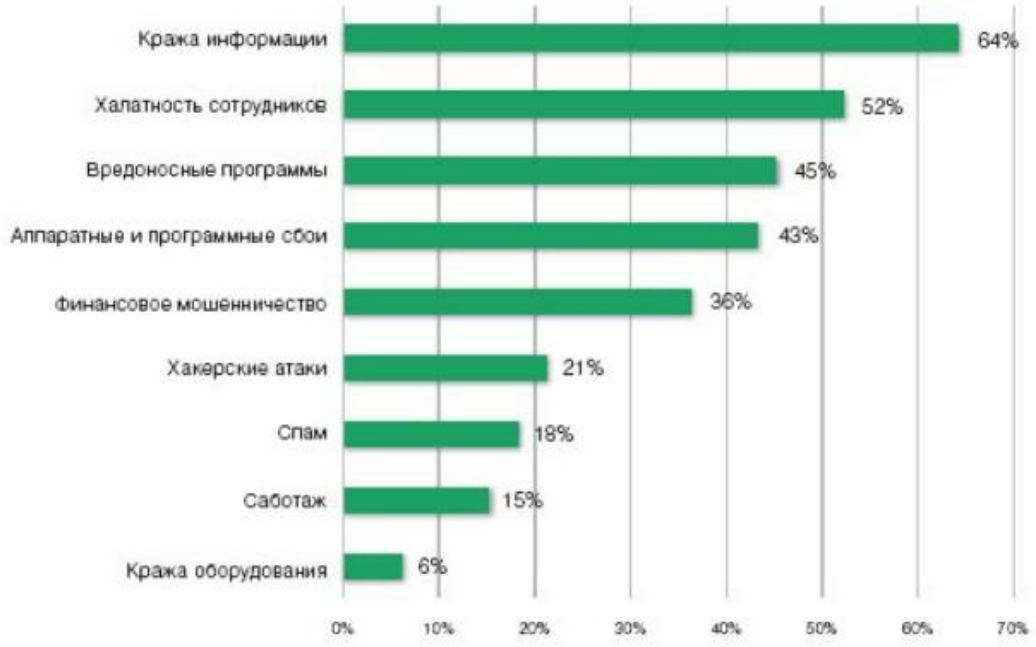

Рисунок 1 – Опасные угрозы информационной безопасности
Источник: «Угрозы информационной безопасности

Использование различных интернет ресурсов, авторизация в сомнительных сайтах с вводом личных данных, согласие на получение рекламной рассылки – все это приводит к сопоставлению вас как нового клиента и позволяет собрать вашу личную информацию более детально. Неудивительно, что защита персональных данных, а также и информационная безопасность волнует потребителей информационных технологий.

Под информационной безопасностью, согласно Федеральному закону, понимается комплекс мер, направленных на защиту информации и поддерживающей ее среды (данные, программные и технические средства) от случайного или преднамеренного разрушения, модификации, раскрытия или потери. [3]

Для обеспечения информационной безопасности государство ведет постоянный контроль и защиту от внешних и внутренних угроз информационного пространства. Существуют различные меры информационные безопасности, которые принимаются для противодействия киберугрозам, однако наиболее эффективным считается применение всего комплекса мер одновременно. К наиболее частым мерам обеспечения безопасности относятся:

- криптографическая защита;
- формирование нескольких уровней защиты от кибератак;
- использование лицензированного программного обеспечения;
- своевременное резервное копирование информации и приложений;
- защита данных.

Криптографическая защита информации подразумевает механизм защиты информации благодаря использованию шифрования данных. Данный метод активно используется в современном мире для хранений, обработки и передачи данных. Важным компонентом данного метода является ключ, который отвечает за выбор и порядок преобразования.

Уровни защиты информации – это совокупность мер, входящих в состав системы защиты информации, применяемых в пределах контура безопасности для реализации защиты информации соответствующей важности. Существует различное число уровней, в зависимости от требования информационной среды, однако основными выделяют четыре [4]:

1. предотвращение – доступ к информации и технологиям предоставляется только персоналу;
2. обнаружение – осуществляется раннее обнаружение преступлений и злоупотреблений, даже при обходе защиты;
3. ограничение – попытки уменьшения потерь, даже если преступление все же было произведено;
4. восстановление – обеспечение восстановления информации при наличии данных, способствующих проведения восстановления.

Несмотря на всевозможные средства обеспечения информационной безопасности, киберпреступники использую более изощренные методы для получения конфиденциальной информации. Наиболее действенные методы по сбору данных со стороны преступников приходятся на менее защищенный элемент системы – человеческий фактор:

- рассылка по организационной почте с вредоносным вложением;
- распространение вредоносного программного обеспечения в интернет ресурсах;
- изъятие данных посредством физического вмешательства.

В независимости от того, в каком виде хранится и передается информация, необходимо реализовывать защитные меры. Именно поэтому, большинство организаций проводят обучение специализированных лиц, которые в дальнейшем работают над усовершенствованием защиты данных. [5-8]

Специалисты информационной безопасности строят и внедряют системы защиты и предотвращают попытки проникновение сторонних лиц, с цельно получения данных. Помимо защиты информации, специалисты предотвращают ошибки и всевозможные баги систем.

Основные требования, предъявляемые к специалисту в области информационной безопасности:

- знание основ криптографии, криптоанализа;
- наличие базовых знаний по компьютерным сетям и сетевым протоколам;
- понимание принципов работы и назначения сетевых устройств;
- знание принципов построения сетей (принципы классификации сетей, принципы работы сетевого оборудования, топология сетей);
- владение основными методами анализа и обнаружения атак.

Более детализировано, требования к специалисту в области информационной безопасности (ИБ), можно описать так:

1. знание российского законодательства в области ИБ, и международных стандартов ИБ (в том числе ISO 27002);
2. знание криптографии и современных средств криптозащиты;
3. умение работать с различными языками программирования (C/C++, C#, Python и пр.);
4. знание операционных систем семейства UNIX;

5. знание технологий защиты web-приложений, информационных систем и сетей передачи данных;
6. опыт работы с системами обнаружения атак и контроля защищенности информационных ресурсов;
7. опыт работы по линии службы безопасности, аудита;
8. знание современных угроз и способов их предупреждения, а также современных средств и методов защиты информации;
9. знание и понимание основ сетевых технологий;
10. знание серверов и систем виртуализации;
11. знание сетевых технологий:

- знание технологии построения сетей передачи данных;
- знание топологий локальных сетей;
- знания стандартов семейства TCP/IP.

12. знание серверных ОС: Linux, Windows Server;
13. знание программ, используемых для проведения аттестации ИСПДн;
14. понимание принципов работы распределенных информационных систем;
15. знакомство с системами обнаружения (предотвращения) несанкционированной деятельности.

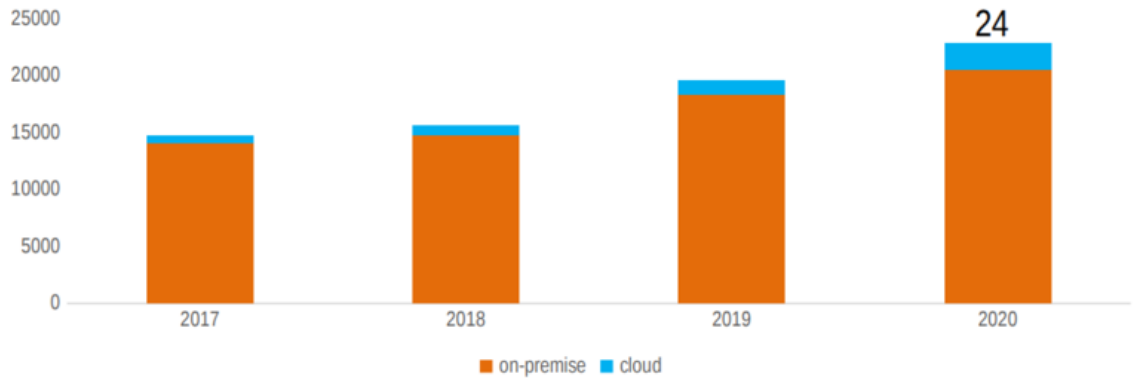

Рисунок 2 – Объем, структура и динамика рынка безопасности
Источник: Tadviser «Безопасность информационных систем»

Безопасность следует воспринимать не как ограничение, а как процесс, общий для любой системы, подверженной угрозам, исходящим от человека, организации, процедур и т. д. Поэтому необходимо интегрировать этот процесс и защитить информационные системы для свободного обмена, хранения и обработки данных.

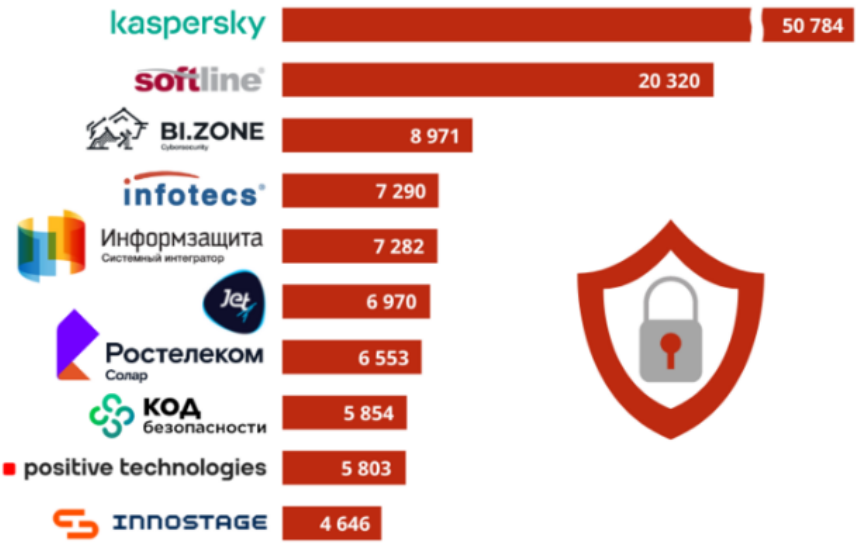

Рисунок 3 – Крупнейшие поставщики решений в сфере информационной безопасности

Источник: Tadviser «Безопасность информационных систем»

Все более миниатюризированная и индивидуализированная система информационных технологий подвергается угрозам, которые исходят от людей, организаций, процедур и устройств в результате ошибок, сбоев, аварий и, прежде всего, в большинстве случаев, из-за злого умысла.

Технические ограничения исчезают; услуги имеют приоритет над инфраструктурой. Сеть теперь «виртуальная» и глобальная; клиент снова становится активным.

Список литературы

1. Белов Е.Б., Лось В.П. Основы информационной безопасности. М. : Горячая линия : Телеком, 2006.
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 3-е изд. М. : Академия, 2008.
3. Абрашев А., Жедрин И., Акулов В. Глобальные тенденции рынка информационной безопасности // Information Security/ Информационная безопасность. 2015. №5. С 16-17.
4. Уровни защиты информации в некредитных финансовых организациях [Электронный ресурс] / Режим доступа: https://inlnk.ru/1PEgRw (Дата обращения: 04.01.2023)
5. Жан-Марк Безопасность информационных систем – гарантия контроля рисков. [Электронный ресурс] / Жан-Марк Режим доступа: https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/securite-des-si-organisation-dans-l-entreprise-et-legislation-42458210/la-securite-des-systemes-d-information-garantir-la-maitrise-du-risque-s8260/ (Дата обращения: 04.01.2023)
6. Политика безопасности информационных систем (ISSP) [Электронный ресурс] / Режим доступа: https://www.dgdr.cnrs.fr/bo/2007/01-07/416-bo0107-pb0.htm (Дата обращения: 04.01.2023)

7. Меры обеспечения информационной безопасности [Электронный ресурс] / Режим доступа: https://inlnk.ru/84ezL7 (Дата обращения: 04.01.2023)
8. Безопасность информационных систем [Электронный ресурс] / Режим доступа: https://inlnk.ru/0QmKlR (Дата обращения: 04.01.2023)

References

1. Belov E.B., Los V.P. Fundamentals of Information Security. M. : Goryachiy liniya : Telecom, 2006.
2. Melnikov V.P., Kleymenov S.A., Petrakov A.M. Information security and information protection. 3rd ed. M. : Akademiya, 2008.
3. Abrashev A., Zhedrin I., Akulov V. Global trends in the information security market // Information Security/ Information security. 2015. №5. S 16-17.
4. Levels of information protection in non-credit financial organizations [Electronic resource] / Access mode: https://inlnk.ru/1PEgRw (Date of access: 04.01.2023)
5. Jean-Marc Information Systems Security is a guarantee of risk control. [Electronic resource] / Zhan-Marc Access mode: https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/securite-des-si-organisation-dans-l-entreprise-et-legislation-42458210/la-securite-des-systemes-d-information-garantir-la-maitrise-du-risque-s8260/ (Date of access: 04.01.2023)
6. Politics of security of information systems (ISSP) [Electronic resource] / Access mode: https://www.dgdr.cnrs.fr/bo/2007/01-07/416-bo0107-pb0.htm (Date of access: 04.01.2023)
7. Measures to ensure information security [Electronic resource] / Access mode: https://inlnk.ru/84ezL7 (Date of access: 04.01.2023)
8. Security of information systems [Electronic resource] / Access mode: https://inlnk.ru/0QmKlR (Date of access: 04.01.2023)