УДК 004.9 **DOI: 10.18413/2518-1092-2021-6-3-0-3**

Воронина А.А.
Скрипина И.И.

ПРЕДУПРЕЖДЕНИЕ ИНЦИДЕНТОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДАННЫХ

Белгородский государственный аграрный университет имени В.Я. Горина, ул. Вавилова, д.1, п. Майский, Белгородский р-н, Белгородская обл., 308503, Россия

e-mail: voronina.anastasia@internet.ru, skripina@bsu.edu.ru

Аннотация
Информация становится очень важным ресурсом и начинает превышать по своей значимости даже материальные активы. В связи со стремительным развитием важности информации в современном мире стали расти и посягательства на информационные ресурсы. Проанализированы средств по защите информации, предотвращающие несанкционированные доступы к ней или ее элементам. Данная группа средств определяется как термин «информационная безопасность». Стоит отметить, что важны именно предупредительные меры для обеспечения безопасности информации, а не устранение последствий данных проблем. В ходе своей работы разработчик может случайно допустить ошибку, вследствие которой в данном пункте может образоваться будущая уязвимость. Уязвимость – слабое место программы или программного обеспечения, обнаружив это место злоумышленник может легко нанести вред информации. Если обнаружена угроза, то применяют методы по обеспечению безопасности информации. В данной статьей рассмотрены меры защиты информации.
Ключевые слова: информационная безопасность, информация, угрозы безопасности.
Для цитирования: Воронина А.А. Скрипина И.И. Предупреждение инцидентов нарушения информационной безопасности данных // Научный результат. Информационные технологии. – Т.6, №3, 2021. – С. 20-25. DOI: 10.18413/2518-1092-2021-6-3-0-3

Voronina A.A.
Skripina I.I.

PREVENTING INFORMATION SECURITY INCIDENTS

Belgorod State Agrarian University named after V.Ya. Gorin, 1 Vavilova St., item Mayskiy, Belgorodsky district, Belgorod region, 308503, Russia

e-mail: voronina.anastasia@internet.ru, skripina@bsu.edu.ru

Abstract
Information is becoming a very important resource and begins to exceed even tangible assets in importance. In connection with the rapid development of the importance of information in the modern world, encroachments on information resources began to grow. A group of information security tools was developed to prevent unauthorized access to it or its elements. This group of tools is defined as the term "information security". It should be noted that it is precisely the preventive measures to ensure the security of information that are important, and not the elimination of the consequences of these problems. In the course of his work, the developer may accidentally make a mistake as a consequence of which a future vulnerability may be formed at this point. Vulnerability is a weak point of a program or software; having discovered this point, an attacker can easily harm information. If the threat came out deliberate, then there are methods to ensure the security of information. This article discusses information protection measures.
Keywords: information security, information, security threats.
For citation: Voronina A.A. Skripina I.I. Preventing information security incidents // Research result. Information technologies – T.6, №3, 2021. – P. 20-25. DOI: 10.18413/2518-1092-2021-6-3-0-1

ВВЕДЕНИЕ

Один из самых динамичных, стремительно формирующихся рынков в мировой экономике – рынок информационных технологий. Раскрывается степень важности исследования в данной ситуации – сила информационных технологий проникает буквально во все сферы человеческой деятельности: информационные технологии внедряются в повседневную жизнь людей, бизнес-процессы компаний и механизмы управления государством. Помимо традиционных материальных, природных и энергетических ресурсов, в условиях усложнения инфраструктуры рынка информационных технологий, формируется еще один стратегический ресурс – информация.

Информация – это уже самостоятельный актив, и она давно преобладает над материальным капиталом. Значительное повышение ценности информации требует внимательного отношения к задаче ее защиты от посягательств. Защитой информации занимается информационная безопасность [1].

Предупреждение возможных информационных атак обеспечивается специальными методами и средствами: от технических средств и программных обеспечений, до нормативных средств защиты в виде документов, правил и мероприятий.

ОСНОВНАЯ ЧАСТЬ

Рассматривая термин «информационная безопасность» в широком понимании, можно сказать, что это средства защиты информации, или чаще всего – группа средств защиты информации, которые предназначены для предотвращения несанкционированного доступа к ней или ее важным элементам [2]. Важно заметить, что правильным подходом к созданию системы информационной безопасности является именно принятие предупредительных мер по обеспечению конфиденциальности, а не устранение последствий [3, 4].

Цепь модификации информации вследствие возможного нарушения безопасности:

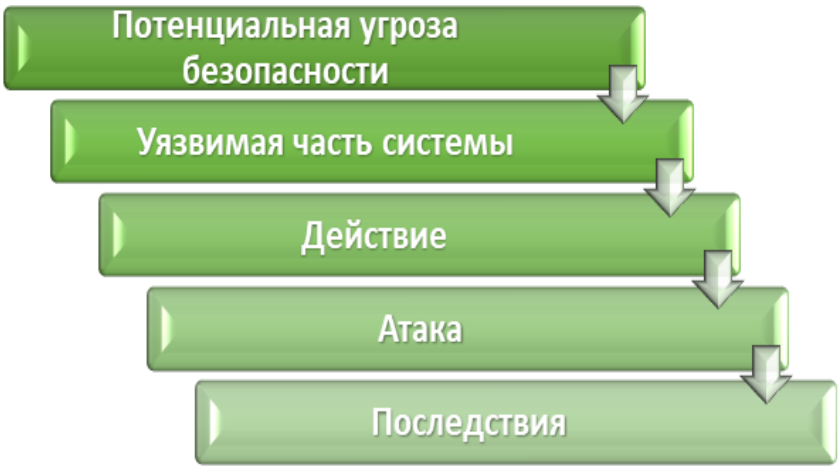

Рис. 1. Модель возможной трансформации информации
Fig. 1. The model of possible transformation of information

Злоумышленники могут использовать полученную конфиденциальную информацию при написании вирусов. Например, один из первых интернет – червей или Morris worm, который был создан Робертом Моррисом, использовал известные уязвимости безопасности для распространения между компьютерами. В следствие было поражено около 10% узлов Арпанета, прототипа современного Интернета. По итогу были введены жесткие нормативы компьютерной безопасности. Данная «эпидемия» наглядно проявила опасность полного доверия компьютерным сетям [5].

В настоящее время по данным крупного портала по теме корпоративной информатизации «TADVISER. Государство. Бизнес. ИТ» в статье об утечке информации указано, что Россия один

из мировых лидеров по количеству умышленных утечек информации – 79,7%. В этом же Интернет-ресурсе отмечено, что около 59% россиян замечали свою персональную информацию в свободном доступе хотя бы единожды [6].

УЯЗВИМОСТИ И РАСПРОСТРАНЕННЫЕ ВИДЫ УЯЗВИМОСТЕЙ

При разработке программного обеспечения программисты могут на любом этапе жизненного цикла ПО допустить ошибку, которая в последствие станет уязвимостью данной программы. Появившаяся уязвимость может позволить злоумышленникам завладеть доступом к функциям и данным системы. Устойчивость к несанкционированному доступу, а также предотвращение возможного появления уязвимости программы, обеспечивает безопасное программирование [7].

Любая программа на компьютере – предположительная цель для злоумышленников. Далее их назначение – найти уязвимость информационной системы, возможную угрозу безопасности, находящейся в ней информации. Существует специальный открытый стандарт CVSS (Common Vulnerability Scoring System), предназначение которого – оценочный расчет уязвимости в безопасности ИС по балльной системе [8].

В стандарте CVVS существует система метрик, позволяющая разделить приоритеты для исправления уязвимостей, всего метрик три, и каждая относится к определенному смысловому разделу.

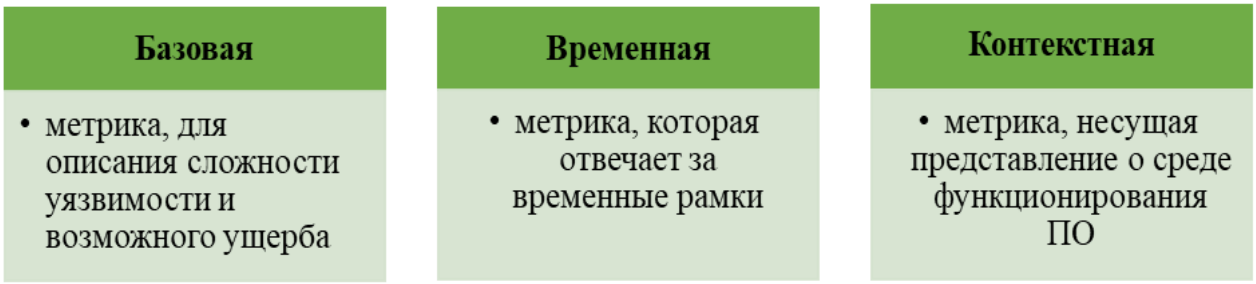

Рис. 2. Метрики, разделяющие приоритеты над уязвимостями
Fig. 2. Metrics that share priorities over vulnerabilities

Рассмотрим в таблице распространенные уязвимости, которые подвергают угрозе безопасность информационных систем:

Таблица 1

Ошибки, ставящие под угрозу безопасность данных

Table 1

Errors that compromise data security

Номер по порядку	Ошибка	Описание ошибки
1	SQL-кодинг	При работе с базами данных необходимо учитывать уязвимости, при которых происходит внедрение SQL в запрос, например, «изменить/добавить данные», при этом злоумышленник может получить доступ к локальным файлам и выполнению команд на взломанном сервере.
2	Переполнение буфера	Некое явление, при котором объем информации, записанной в ячейку памяти, превышает

Номер по порядку	Ошибка	Описание ошибки
		выделенный, что в итоге наносит возможную угрозу данным.
3	Арифметическое переполнение	Ситуация, при которой вследствие каких-либо арифметических действий размер результата превышает максимально возможное значение переменной.
4	Состояние гонки (конкуренция)	Ошибка, в результате которой работа приложения будет завесить от порядка частей кода. Также к данному понятию можно применить термин неопределённость параллелизма.
5	Слабые пароли	В большинстве случаев пользователи не придают особое значение паролям, используя простые и предсказуемые комбинации.
6	Сокрытие трафика	Различные зашифрованные туннели в виде Tor, VPN и т.д. могут служить инструментами для сокрытия трафика. Использование данных туннелей приводит к занижению средств защиты.
7	Неудачный выбор алгоритма шифрования	Каждый алгоритм шифрования будет иметь свои плюсы и минусы. Необходимо использовать симметричное шифрование в группе с ассиметричным.

В настоящее время список уязвимостей пополняется ежедневно, поэтому указать абсолютно все известные уязвимости просто невозможно. Вышеприведенный список уязвимостей включает в себя самые популярные ошибки, последствия которых могут быть трагичными.

МЕТОДЫ ЗАЩИТЫ ОТ ОШИБОК И УЯЗВИМОСТЕЙ

Важным элементом защиты от ошибок и уязвимостей является постоянный контроль и проверка входных данных.

Рассмотрим ошибку, связанную с переполнением буфера, наилучшим вариантом защиты от превышения выделенных размеров памяти – проверка, что данные действительно не превышают объемов буфера.

В проверке нуждаются данные, которые будут отправлять в БД, для защиты от атаки внедрения SQL – кода. Однако, если проводить излишнее число проверок, это может усложнить разработку исходного кода и привести к новым ошибкам. Поэтому, стратегию контроля и проверки данных следует совмещать с другими стратегиями.

Компиляторы тоже могут выступать в качестве различных механизмов для защиты от уязвимости. Microsoft Visual C++ – компилятор, предназначенный для разработки на языке C++, позволяет еще находясь на этапе компиляции проверить данные на арифметическое переполнение.

В помощь контролю процесса исполнения программы может вступить и операционная система. Существует специальная технология рандомизации схемы адресного пространства, она может быть применима в тех случаях, когда исходный код неизвестен. Данная технология предотвращает запуск произвольного кода.

ЗАКЛЮЧЕНИЕ

В заключение можно отметить, что обеспечение информационной безопасности является важной частью работы над программным продуктом и при разработке приложений, программных обеспечений и информационных систем уделяют немаловажное значение уязвимостям. Принято считать, что во избежание ошибок и потерь данных необходимо проводить тщательный анализ возможных уязвимостей. Однако, не стоит полагаться только на один способ защиты, всегда необходимо руководствоваться случаями в конкретной ситуации и действовать комплексными подходами, следует изучить наиболее опасные уязвимости и быть готовыми к возможной атаке, если злоумышленникам все же удалось нарушить процесс безопасности - необходимо зафиксировать случай уязвимости, чтобы избежать их в дальнейшем.

Список литературы

1. Зубкова Т.М. Технология разработки программного обеспечения: учебное пособие; Оренбургский гос. ун-т. – Оренбург: 1 ОГУ, 2017. 468 с.
2. Зенков А.В. Информационная безопасность и защита информации: учебное пособие для вузов / А.В. Зенков. — Москва: Издательство Юрайт, 2021. 104 с.
3. Величко М.С., Маслова М.А. Информационная безопасность как услуга в новом дистанционном мире // Научный результат. Информационные технологии. Т.5. №4, 2020. – С. 31-36. DOI: 10.18413/2518-1092-2020-5-4-0-5.
4. Нестеренко В.Р., Маслова М.А. Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними // Научный результат. Информационные технологии. – Т.6, №1, 2021. – С. 48-54. DOI: 10.18413/2518-1092-2021-6-1-0-6.
5. Теория информационной безопасности и методология защиты информации / Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.
6. Ибодуллаева З., Нурметова Б.Б. Информационная безопасность: угрозы и методы защиты // Студенческий: электрон. научн. журн. 2019. № 20(64). URL: https://sibac.info/journal/student/64/143596 (дата обращения: 13.08.2021).
7. Артюхин Д.Р. Информационная безопасность предприятий // Студенческий электрон. научн. журн. 2020. № 31(117). URL: https://sibac.info/journal/student/117/188433 (дата обращения: 12.08.2021).
8. ЛК сопоставляет опасения российских компаний со статистикой реальных утечек, 2020 г. URL: https://www.anti-malware.ru/news/ (дата обращения 08.08.2021)

References

1. Zubkova TM Software development technology: a tutorial; Orenburg state un-t. – Orenburg: 1 OSU, 2017. 468 p.
2. Zenkov, A.V. Information security and information protection: a textbook for universities / A.V. Zenkov. – Moscow: Yurayt Publishing House, 2021.104 p.
3. Velichko M.S., Maslova M.A. Information security as a service in the new remote world // Research result. Information technologies. – T.5. №4, 2020. – P. 31-36. DOI: 10.18413/2518-1092-2020-5-4-0-5.
4. Nesterenko R.V., Maslova M.A. Modern challenges and threats information security public cloud making and methods of work with them // Research result. Information technologies. – T.6, №1, 2021. – P. 48-54. DOI: 10.18413/2518-1092-2021-6-1-0-6.
5. Information security theory and information protection methodology / Gatchin Yu.A., Sukhostat V.V, Kurakin A.S., Donetskaya Yu.V. – 2nd ed., Rev. and add. – SPb: ITMO University, 2018. – 100 p.
6. Ibodullaeva Z., Nurmetova B.B. Information security: threats and protection methods // Student: electron. scientific. zhurn. 2019. No. 20 (64). URL: https://sibac.info/journal/student/64/143596 (date access: 13.08.2021).
7. Artyukhin D.R. Information security of enterprises // Student electronic scientific journal. 2020. No. 31(117). URL: https://sibac.info/journal/student/117/188433 (date access: 12.08.2021).
8. LK compares the fears of Russian companies with statistics of real leaks, 2020. URL: https://www.anti-malware.ru/news/ (date access: 08.08.2021)

Воронина Анастасия Александровна, студентка кафедры математики, физики, химии и информационных технологий
Скрипина Ирина Ивановна, преподаватель кафедры математики, физики, химии и информационных технологий

Voronina Anastasia Aleksandrovna, Student of the Department of Mathematics, Physics, Chemistry and Information Technologies
Skripina Irina Ivanovna, Lecturer of the Department of Mathematics, Physics, Chemistry and Information Technologies