УДК 004.43 **Технические науки**

Фадеева Ксения Андреевна, *студентка ФДО и СПО ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва», г. Саранск*

Хамидуллова Динара Рамильевна, *студентка ФДО и СПО ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва», г. Саранск*

Прокин Александр Александрович, *преподаватель, «Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва», г. Саранск*

ПУТИ СНИЖЕНИЯ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ ЕГО РАЗРАБОТКЕ

Аннотация: Разработка современного программного обеспечения предполагает не только реализацию функциональных возможностей этого ПО, но и снижение уязвимостей для его дальнейшей безопасной эксплуатации.

Путь по снижению уязвимости программного обеспечения начинается с описания наиболее известных рисков и дальнейшей их нейтрализации. Данная статья освещает распространенные риски, которым подвержены современные информационные системы, и эффективные меры по их анализу, оценке, предупреждению и частичному или полному предотвращению.

Ключевые слова: угрозы, уязвимости, информационная система, программное обеспечение.

Annotation: The development of modern software involves not only the implementation of the functionality of this SOFTWARE, but also the reduction of vulnerabilities for its further safe operation.

The way to reduce software vulnerability begins with a description of the most known risks and their further neutralization. This article highlights the common risks to which modern information systems are exposed, and effective measures for their analysis, assessment, prevention and partial or complete prevention.

Keywords: threats, vulnerabilities, information system, software.

Меры по обеспечению информационной безопасности программного продукта (далее ПП) должны быть экономически выгодными для заказчика. Данная статья освещает наиболее эффективные методики, которые позволяют предугадать возможные затраты на предотвращение потерь в следствии нарушений информационной безопасности и результативно сконцентрировать основные экономические ресурсы в данных направлениях.

Для правильного выбора необходимых экономичных средств обеспечения безопасности следует изучить возможные угрозы, которые обычно эксплуатируют уязвимые места разрабатываемой системы.

Процесс, во время которого возникает потенциальная возможность нарушения информационной безопасности, называется угрозой. Под атакой следует понимать попытку осуществления определенной угрозы, а того, кто предпринимает данные действия – злоумышленником. Зачастую его называют источником угрозы. Также в данном контексте следует затронуть термин «уязвимость».

Существует много разных определений «уязвимости», охватывающих различные области применения, которые включают в себя атаки, риски, намерение, угрозы. В данной статье мы определяем уязвимость как одну или несколько слабых сторон программного обеспечения, нарушение работы которой могут быть вызваны случайно или умышленно и привести к сбою системы [1]. Программный продукт, созданный для определенного заказчика в любом случае, будет в какой-то мере уязвим. Причины этой уязвимости весьма очевидны:

– ненадежность платформы, на которой разрабатывается и функционирует программное обеспечение (далее ПО);

– внешние модули, подключаемые к ПО также ненадежны;

– реорганизация процесса разработки;

– недостаточная продуманность процесса обновления программного продукта;

– непосредственно недоработки команды программистов в отношении написания кода: непонятность кода для других программистов в случае передачи проекта другим разработчикам, отсутствие проверки ввода и вывода данных, некорректное документирование и комментирование кода.

– ограниченные сроки, предоставленные для реализации программного продукта;

– бесконечное изменение требований со стороны заказчика.

Уязвимость в области защиты информационных систем (например, несанкционированный доступ к ошибке в программном или аппаратном обеспечении) чаще всего подвержена угрозам. Период времени между моментами использования уязвимости и её устранения, называют окном опасности. Успешная атака возможна только в период, когда существует окно опасности. Срок существования окна опасности для большинства уязвимостей может достигать длительного времени (от нескольких дней до нескольких недель). За это время система должна пройти несколько этапов обнаружения и исправления уязвимостей:

– идентификация уязвимости;

– разработка соответствующих мер по устранению уязвимостей;

– применение данных мер в области системы, которая подвержена влиянию угроз.

Процесс появления новых уязвимостей цикличен, т.е. в любой разрабатываемой системе имеются окна опасности и периодически появляются новые. Мониторинг данного процесса должен осуществляться непрерывно, а разработка и применение соответствующих мер по его устранению –

максимально быстро. Не всегда и не все угрозы – результат допущенных ошибок и подсчётов [1]. Некоторые из них имеют место быть априори (например, возможность отключения электроэнергии, в следствии чего – выход параметров за допустимый диапазон).

Существует множество мифов о распространённых угрозах и уязвимостях, которые влияют на современных информационные системы. Незнание зачастую приводит к превышению допустимого бюджета или, в худшем случае, нецелесообразное направление ресурсов в область, которая в них не нуждается. Следует обратить внимание на то, что термин «Угроза» в разных ситуациях формулируется по-разному. Например, система, разработанная для организации, в которой данные имеют открытый доступ не подвержена риску конфиденциальности. Однако, чаще всего, неправомерный доступ является серьезной угрозой.

Искоренить подверженность программного продукта данным рискам невозможно, но можно минимизировать их с помощью качественной организации разработки.

С точки зрения среднестатистической организации угрозы можно квалифицировать следующим образом:

– местоположение источника угроз относительно рассматриваемого ПП;

– компонент, который является целевым направлением угрозы (данные, программы, аппаратура, поддерживающая инфраструктура);

– метод реализации угроз (случайные или преднамеренные действия определенного характера);

– определенный результат, который в итоге должен быть получен вследствие воздействия угрозы (основной критерий).

С финансовой точки зрения (размер ущерба) чаще всего встречаются такие ошибки непреднамеренного характера, которые допускают штатные пользователи, операторы, системные администраторы, обслуживающие систему. Именно такие ошибки становятся непосредственной угрозой для системы, в некоторых случаях они создают уязвимости, которые вследствие

могут стать целью злоумышленников [2]. По среднестатистическим данным около 65% потерь являются результатом ошибок непреднамеренного характера. Результат неорганизованности и безграмотности обслуживающего персонала зачастую влечет за собой больше последствий чем, допустим, пожары и наводнения. Чтобы избежать таких непреднамеренных ошибок, необходимо принять радикальные меры – жесткий контроль, который подразумевает под собой максимально допустимую правильность совершаемых действий, применение метода автоматизации рабочего процесса.

Также угрозы доступности можно классифицировать по определенным компонентам информационной системы, которые являются целью для угроз:

– отказ пользователей;

– отказ внутри информационной системы;

– отказ инфраструктуры, занимающейся поддержкой информационной системы.

В первом случае отказ пользователей происходит по следующим причинам:

1. Пользователи не хотят работать с информационной системой, так как зачастую не желают осваивать новые технологии или же их запросы не соответствуют техническим характеристикам.

2. Пользователи не обладают достаточной компьютерной грамотностью, не умеют работать с документацией и т.д.

3. Отсутствие необходимой технической поддержки.

Отказ внутри информационной системы возникает из-за:

1. Не соблюдений правил эксплуатации информационной системы.

2. Не корректное переконфигурирование системы.

3. Отказ программного и аппаратного обеспечения.

4. Нарушение целостности данных.

5. Повреждение аппаратуры

В случае отказа поддерживающей инфраструктуры могут возникнуть следующие угрозы:

1. Нарушения в работе систем связи, электро-, водо- и теплоснабжения.

2. Нарушение целостности помещений

3. Не выполнение персоналом по обслуживанию системы или пользователями своих обязанностей.

Не менее опасными являются случаи, когда уволенные сотрудники преднамеренно наносят вред системе из-за личностных конфликтов с организацией. В этом случае лучше всего при увольнении сотрудника аннулировать права доступа к ресурсам информационной системы. Стихийные события разрушающего характера (пожары, наводнения, землетрясения и т.д.) также являются опасными для работы системы. 13% потерь, нанесенных информационным системам, приходится на данный вид угроз.

Внедрение в информационные системы вредоносного программного обеспечения является одним из самых опасных видов атак.

Можно выделить следующие аспекты вредоносного программного обеспечения:

– функция, которая является вредоносной;

– способ распространения;

– внешнее представление.

Функция не всегда вся является вредоносной. Зачастую в этой функции существует некая часть, которая непосредственно наносит вред системе. Такие фрагменты функций могут характеризоваться разными уровнями сложной логики, но обычно они предназначены для выполнения следующих задач:

– внедрения в систему другого программного обеспечения;

– получение доступа к атакуемой системе для осуществления контроля над ней;

– последующее нарушение целостности и работоспособности программы или данных.

Также вредоносные функции можно классифицировать по механизму распространения:

– вирусы – это специальный код, который способен внедряться в другие программы;

– «черви» – это специальный код, который способен распространять свои копии и выполнять их в системе без внедрения в какие-либо части системы.

Необходимо отметить, что данные определения и классификации вредоносного программного обеспечения, которые приведены в статье отличаются от тех, что описаны в ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения": "Программный вирус — исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах"[3].

Разработка информационных систем и дальнейшее их использование подразумевает под собой совокупность рисков. Когда возможный ущерб, нанесенный вредоносными программами и функциями сравнительно велик, то следует принять меры защиты, которые являются экономически выгодными. В данном случае необходимо периодические анализ и оценка рисков для контроля безопасности системы.

Под размером риска с количественной точки зрения понимают функцию вероятности реализации определенной угрозы и размер предполагаемого ущерба.

Следовательно, над рисками производится работа по их управлению, позволяющая произвести оценку размера рисков, разработать план эффективных мер по минимизации ущерба и осуществить проверку приемлемых границ, которые установлены для рисков.

Чаще всего наиболее распространенные риски известны как разработчику, так и персоналу, который осуществляет администрирование данной системы. На практике, к сожалению, количество угроз превышает ожидаемые, и не каждая из них носит компьютерный характер. Так, например,

угрозой могут выступать внешние вредители (мыши, тараканы и т.д.) в помещениях организации. Мыши могут нанести вред кабелям, а тараканы – вызвать короткое замыкание.

Наличие угроз информационной системы обуславливается её уязвимостями в системе безопасности, которые характеризуются недостатками защитных механизмов [4].

Первым этапом в процессе анализа угроз является их идентификация. Необходимо провести максимально полное рассмотрение анализируемых видов угроз. Источниками возникновения этих угроз также могут повлиять на выбор дополнительных средств защиты, поэтому необходимо уделить им особое внимание.

Следующим этапом после идентификации будет являться оценка вероятности осуществления угроз. В данном случае для оценки используется трёхбалльная шкала (низкая (1), средняя (2) и высокая (3) вероятность).

Не менее важным является размер предполагаемого ущерба, который также оценивается по трёхбалльной шкале. Под оценкой размера ущерба следует понимать не только расходы, требуемые для замены поврежденного оборудования и восстановление информации, но и средства, необходимые для восстановления репутации компании.

После сбора всех необходимых исходных данных и оценки степени неопределенности следует перейти к следующему этапу – оценки рисков. Если идентификация рисков и оценка их потенциальных размеров ущерба оценивается по трёхбалльной шкале, то данный процесс следует оценивать по такому типу:1,2,3,4,6 и 9. Если оценка сводится к 1 или 2 баллам, то такие риски можно отнести к низким, если же результат оценивания – 3 или 4 балла, то это средние риски, а к высоким относят риски, оцениваемые в 6 и 9 баллов. По данной шкале оцениваются приемлемость рисков.

Принять дополнительные меры по защите системы будет необходимым, если риски оказались недопустимо высокими. Обычно для нейтрализации уязвимости, ставшей причиной опасной угрозы, существует несколько особо

эффективных и экономически выгодных механизмов безопасности. Так, например, для входа в систему пользователям предлагается выбрать длинный пароль, что поможет избежать вероятности нелегального входа в систему.

Схематически этапы анализа и оценки рисков представлены на рисунке 1.

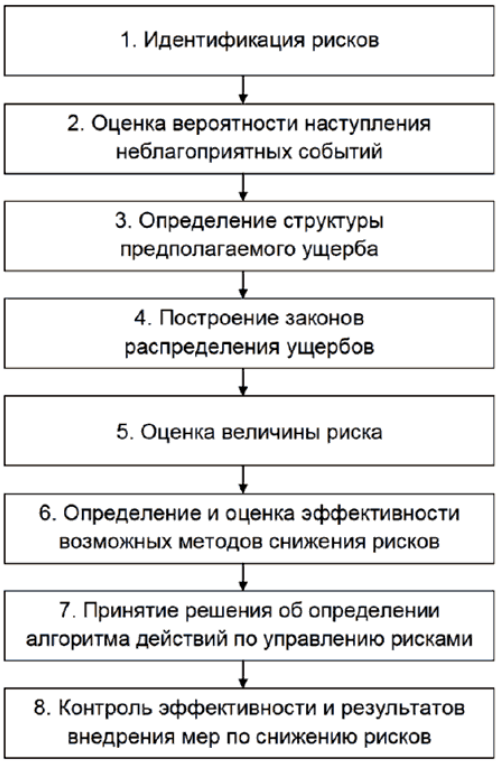

Рисунок 1 – Этапы анализа и оценки рисков

В данной статье были рассмотрены основные виды рисков и эффективные методы по их управлению: оценка, анализ и принятие решений. Главная особенность управления рисками заключается в том, что к каждому из них требуется уникальный подход, так как не существует готовых и универсальных методов и решений проблемы уязвимости и устранения угроз.

Основной задачей персонала, обслуживающего систему, является подбор наиболее эффективных и подходящих решений – оценка и минимизация риска для получения максимальной прибыли в удачном случае и минимальных потерь в неудачном. Так как влияние некоторых факторов может разрушить работу целой компании, то возникает потребность в опытных и высококвалифицированных руководителях. С их стороны своевременно должен

осуществляться анализ существующей ситуации, при котором важно использовать опыт организаций, ранее сталкивающихся с такими ситуациями.

В заключении можно сказать, что грамотное и эффективное определение направлений развития фирмы – залог своевременного предотвращения возможных уязвимостей

В заключении можно сказать, что своевременное и эффективное предотвращение рисков, в следствии, уязвимостей – залог успешной и прибыльной работы системы.

Библиографический список:

1 Авдеева Я. А., Прокин А. А. Модель памяти в языках программирования [Электронный ресурс] // E-Scio: Электронное периодическое издание «E-Scio.ru». – Режим доступа: http://e-scio.ru/wp-content/uploads/2019/01/%D0%90%D0%B2%D0%B4%D0%B5%D0%B5%D0%B2%D0%B0-%D0%AF.-%D0%90.-%D0%9F%D1%80%D0%BE%D0%BA%D0%B8%D0%BD-%D0%90.-%D0%90.pdf.

2 Прокин А. А., Баландин И. А. Способы тестирования учебных программ [Электронный ресурс] // E-Scio: Электронное периодическое издание «E-Scio.ru». – Режим доступа: http://e-scio.ru/wp-content/uploads/2019/03/%D0%9F%D1%80%D0%BE%D0%BA%D0%B8%D0%BD-%D0%90.-%D0%90.-%D0%91%D0%B0%D0%BB%D0%B0%D0%BD%D0%B4%D0%B8%D0%BD-%D0%98.-%D0%90.pdf.

3 ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. — Введ. 2000-01-01 — М.: Изд-во стандартов, 1999. – 9с.

4 Хамидуллова Д. Р., Фадеева К. А., Макаров В. Э. Брандмауэры, как один из способов защиты информации [Электронный ресурс] // Постулат: Электронное периодическое издание «Постулат». – Режим доступа: http://e-postulat.ru/index.php/Postulat/article/view/1603/1637.