МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**
Кафедра математической кибернетики и компьютерных наук

МЕТОДЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ ВЗЛОМА НА ПРИМЕРЕ МАКЕТА ИГРЫ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 5 курса 551 группы
направления 09.03.04 — Программная инженерия
факультета КНиИТ
Калентьева Дмитрия Александровича

Научный руководитель
к. т. н., доцент _____ Д. Ю. Петров

Заведующий кафедрой
к. ф.-м. н., доцент _____ С. В. Миронов

Саратов 2021

ВВЕДЕНИЕ

Актуальность темы.

С появлением интернета получение и обмен информацией с каждым днем все набирает обороты. Современный мир уже не способен существовать без вычислительных сетей и «глобальной паутины». Этот факт скрывает за собой не только общедоступность огромного объема информации, быстрого и легкого обмена информацией между пользователями, но и уязвимость информационных данных, которые по тем или иным причинам не должны попасть в третьи руки.

Увеличение объемов данных требует современных решений по их обработки, хранению и защите. Рост вычислительной техники тоже не стоит на месте. Если ранее обработка огромного блока информации была невозможной или занимала несоизмеримо большой промежуток времени, то с увеличением мощности ЭВМ такие операции могут выполняться практически мгновенно (либо за очень короткий промежуток времени). Изобретения новых алгоритмов обработки и защиты данных увеличивает и возможности перехвата этой информации.

В настоящее время информация очень ценный продукт, как по содержанию, так и по цене. Актуальность написания новых, более сбалансированных и быстрых, алгоритмов по обработки и защите данных никогда не спадет, а значит и не спадет интерес завладеть или изменить информацию. Например, огромные корпорации готовы купить ту или иную информацию о продукте конкурента (формулы, составы, патенты, расчеты) как напрямую у конкурирующей фирмы, так и с третьих рук (хакеры).

На примере игровой индустрии (в частности, онлайн игр) мы можем наблюдать «извечное противостояние» разработчиков игр и разработчиков «читов» (стороннего программного обеспечения). Для разработчиков игр или их издателей взлом и манипуляции с игровыми данными влекут за собой увеличение релевантных затрат и уменьшение релевантной прибыли, а также репутационные риски (потеря инвесторов, потеря доверия в будущих проектах). Увеличивающаяся конкуренция в игровой индустрии заставляет разработчиков подходить к защите и сохранности своих данных более тщательно и продумано. В противовес этому, разработчикам стороннего ПО, приходится изобретать новые и улучшать старые «пути обхода».

Актуальность настоящей дипломной работы обуславливается необходимостью решения таких проблем, как: перехват и изменение данных, несанкционированный доступ к персональной информации, а также невозможностью реализации 100% защиты.

Таким образом, довольно оправданным следует посвящение данной работы исследованию и использованию на практике, а именно на примере макета игры, методов защиты программного обеспечения, которые бы обеспечивали решение обозначенных выше задач связанных с безопасностью персональных данных. Поэтому тема выпускной квалификационной работы носит название «Методы защиты программного обеспечения от взлома на примере макета игры».

Цель бакалаврской работы — определение, изучение и понимание методов, с помощью которых возможно получить, изменить и использовать данные в «корыстных целях». Так же реализация методов и алгоритмов, которые поспособствуют предотвращению несанкционированных действий со стороны злоумышленника. Определение целесообразности использования тех или иных способов в реальных условиях.

В соответствии с поставленной целью были определены **следующие задачи:**

1. определение и изучение способов и методов несанкционированного доступа;
2. определение векторов атак (уязвимые места в программном обеспечении);
3. сбор информации для анализа атак;
4. реализация методов для предотвращения несанкционированного доступа.

Практическая значимость бакалаврской работы. Все предложения, предлагаемые при решении задач, могут быть использованы на практике.

Структура и объём работы. Бакалаврская работа состоит из введения, двух глав, заключения, библиографии и приложений. Общий объём работы — 78 страниц, из них 46 страниц — основного материала, 79 рисунков, 4 приложения, 1 автореферат, 1 задание на бакалаврскую работу, 1 отзыв руководителя, 1 отзыв оппонента.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Первый раздел «Основы защиты программного обеспечения во время выполнения и векторы атак» посвящен теоретико-методологическим основам защиты программного обеспечения, рассматривается криптография как основа защиты ПО, эффективность применения и методы использования. Так же рассматриваются способы и методы атак на программное обеспечение со стороны злоумышленников.

Второй раздел «Методы защиты программного обеспечения от взлома на примере макета игры» посвящен рассмотрению возможных и актуальных способов сбора общей системной информации на максимально низком уровне операционной системы для `usermode`-приложений. Описываются методы для обработки и анализа собранной информации, а также способы обнаружения стороннего программного обеспечения. Так же рассматриваются и реализуются методы сокрытия методов работы собственного кода, для затруднения анализа и реверс-инжинеринга со стороны злоумышленника. Реализуется способы защиты игровых переменных от динамического анализа (поиск «точных значений» в выполняемой памяти игры).

ЗАКЛЮЧЕНИЕ

В ходе данной работы было выполнено:

1. определение методов несанкционированного доступа;
2. определение векторов атак;
3. определение и описание методов для предотвращения и анализа несанкционированного доступа;
4. реализация методов по защите строк, переменных и исполняемого кода;
5. реализация методов обнаружения брейкпоинтов и защита от запуска отладчика;
6. реализация методов защиты от запуска стороннего ПО.

Это в свою очередь позволило достигнуть поставленной цели, заключающейся в определении, изучении и понимании методов, с помощью которых возможно получить, изменить и использовать данные в «корыстных целях», а также в реализации методов и алгоритмов, которые поспособствуют предотвращению несанкционированных действий со стороны злоумышленника. При

этом была определена целесообразность использования тех или иных способов в реальных условиях и разработано необходимое программное обеспечение, исходный код которого представлен в приложениях А, Б, В и Г.

Разобрав основные методы несанкционированных атак на защищаемые процессы и на основе собранных и обработанных данных можно сделать вывод, что защитится от атак «зловреда» возможно зная его методы работы при этом не жертвуя оптимизацией и быстродействием защитного кода.

С другой же стороны не зная алгоритмы работы вредоносного программного обеспечения нам потребуется гораздо больше времени на анализ и реализацию алгоритмов защиты, при этом стоит учитывать общую оптимизацию защитного кода и среднестатистическую мощность конечного потребителя.

На основе проведенного анализа источников можно определить, что по статистике более 60% пользователей онлайн игр сталкиваются с нечестной игрой со стороны других игроков. По этой причине разработка новых и более совершенных алгоритмов обнаружения вредоносного программного обеспечения и несанкционированных атак является актуальной темой для разработчиков систем безопасности и разработчиков игр.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Shaikh, S.-A. Intricacies of software protection: a techno-legal review / S.-A. Shaikh, B. Londhe // Journal of Intellectual Property Rights. — 2016. — Vol. 21. — Pp. 157–165.
2. Rasch, A. The impact of piracy on prominent and non-prominent software developers / A. Rasch, T. Wenzel // Telecommunications Policy. — 2015. — Vol. 39, no. 8. — Pp. 735–744.
3. Sander, T. On software protection via function hiding // International Workshop on Information Hiding / Springer. — 1998. — Pp. 111–123.
4. Mana, A. An ef?cient software protection scheme // IFIP International Information Security Conference / Springer. — 2001. — Pp. 385–401.
5. Schaumueller-Bichl, I. A method of software protection based on the use of smart cards and cryptographic techniques // Workshop on the Theory and Application of of Cryptographic Techniques / Springer. — 1984. — Pp. 446–454.
6. Абдулаев, А. А. Защита от компьютерных угроз на основе контроля

опасных событий / А. А. Абдулаев, А. Р. Кадыров, Г. Дамирбек // Современные проблемы механики. — 2018. — № 34. — С. 48–56.

7. Бутакова, Н. Г. Анализ интеграции средств мониторинга и аудита информационной безопасности корпоративной сети / Н. Г. Бутакова, А. А. Трунова // REDS: Телекоммуникационные устройства и системы. — 2017. — Т. 7, № 4. — С. 534–538.
8. Дровникова, И. Г. Анализ типовых сетевых атак на автоматизированные системы органов внутренних дел / И. Г. Дровникова, Е. С. Овчинникова, В. В. Конобеевских // Вестник Дагестанского государственного технического университета. Технические науки. — 2020. — Т. 47, № 1. — С. 117–124.
9. Зубков, Д. А. Анализ компьютерной сети на возможность проникновения и последующая защита с помощью прикладного ПО / Д. А. Зубков // Современные технологии в науке и образовании-СТНО-2020. — 2020. — С. 149–158.
10. Иванова, Д. С. Минимизация угроз утечки конфиденциальной информации организации / Д. С. Иванова // Молодежный исследовательский потенциал. — 2021. — С. 42–50.
11. Куликов, Г. Г. Программно-аналитический комплекс оперировании с множеством реальных и виртуальных объектов по правилам декартово замкнутой логики в информационном пространстве предметной области / Г. Г. Куликов // Информационные технологии и системы. — 2019. — С. 217–222.
12. Купряшин, В. В. Порядок действий по защите информационных систем персональных данных и анализ современных средств защиты от несанкционированного доступа / В. В. Купряшин, Д. В. Аксельрод, А. Н. Якубович // Актуальные проблемы современной когнитивной. — 2018. — С. 74–79.
13. Левшун, Д. С. Проблемные вопросы информационной безопасности киберфизических систем / Д. С. Левшун // Информатика и автоматизация. — 2020. — Т. 19, № 5. — С. 1050–1088.
14. Любимов, А. Разработка рекомендаций по реагированию на инциденты несанкционированного доступа в системе сбора, анализа и мониторинга событий ИБ (siem) / А. Любимов // Информационные технологии в науке,

бизнесе и образовании. — 2017. — С. 44–49.
15. Оладько, В. С. Формализация процедуры аудита подсистемы управления доступом в информационной системе / В. С. Оладько // Моделирование, оптимизация и информационные технологии. — 2019. — Т. 7, № 3. — С. 37–37.
16. Поздняков, А. А. Определение оптимального алгоритма выявления попыток несанкционированного доступа к эксплуатируемой информационной системе / А. А. Поздняков // Инновационные механизмы решения проблем научного развития. — 2019. — С. 44–46.
17. Разумников, С. В. Методика поддержки принятия решений при выборе облачных ИТ-сервисов для внедрения на предприятии / С. В. Разумников // Научные труды Вольного экономического общества России. — 2018. — Т. 212, № 4. — С. 56–62.
18. Ткаченко, В. А. Контроль изменения параметров объектов информационных систем цифровой экономики при осуществлении к ним несанкционированного доступа / В. А. Ткаченко, В. Р. Печенкин // Электронный сетевой политематический журнал «Научные труды КубГТУ». — 2018. — № 6. — С. 958–967.
19. Чженбин, Х. Управление ресурсами распределенной компьютерной системы с учетом уровня доверия к вычислительным компонентам / Х. Чженбин // Кибернетика и системный анализ. — 2017. — С. 189–194.