УДК 004.056 + 004.738.5 Вестник УрФО № 3(37) / 2020, с. 59–68

Анфиногенов М. В., Антясов И. С.

DOI: 10.14529/secur200307

ЭВОЛЮЦИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ВИДЕОИГРАХ

В статье рассмотрены видеоигры как уникальное явление в информационной среде, развитие технологий защиты и методов несанкционированного доступа в видеоигровой индустрии со времен появления первой видеоигры и начала становления индустрии до настоящего времени. Представлены поэтапное изменение систем взаимодействия с видеоиграми, технические особенности как аппаратной, так и программной защиты, которые использовали разработчики видеоигр и компании, производящие платформы для них. Изучены приёмы и методы взлома этих систем защиты, инциденты мировых масштабов. Показано, как ошибки и недочёты в безопасности предыдущих поколений видеоигровых приставок повлияли на становление и развитие систем безопасности в последующих поколениях. Рассмотрен процесс централизации и обобщенности систем обеспечения сохранности данных пользователей в современном мире.

Ключевые слова: *система защиты информации, видеоигра, программная защита информации, аппаратная защита информации, система безопасности, нелицензионное программное обеспечение.*

Anfinogenov M. V., Antyasov I. S.

EVOLUTION OF INFORMATION SECURITY SYSTEMS IN VIDEO GAMES

This article covers the video games as a unique phenomenon in the information environment, the development of security technologies and unauthorized access methods since the first video game release until the position of the video game industry in our time. Represented a step change in the interaction systems, the technical features of both hardware and software security which were used by video game developers and companies producing platforms. The analysis of the hacking techniques and methods intended for these protection systems and related global incidents is made. Illustrated the formation and development of security systems of the video game consoles of subsequent generations under the influence of the mistakes and shortcomings in the data security of the prior console generations. The process of centralization and generalization of the user data integrity systems in the modern world is considered.

Keywords: *information security system, video game, software information security, hardware information security, safety system, unlicensed software.*

Видеоигровая индустрия на данный момент является крупнейшей медиаиндустрией в мире с годовым оборотом в $148.8 млрд, а системы защиты в видеоиграх очень комплексны и разнообразны, но так было далеко не всегда. Первая видеоигра возникла в 1940 году. Это был игровой автомат Nimatron, который представлял собой электронно-релейную машину для игры в «Ним», где игрок гасит лампы в определенном порядке по очереди с компьютером (рис. 1). Кто погасит последнюю лампу – выигрывает. Данный автомат не был коммерческим, а был скорее демонстрационным. Устройство работало на релейной схеме, и создатель Эдвард Кондон продемонстрировал его на всемирной выставке «Мир Завтрашнего дня» в Нью-Йорке. Он рассчитывал на то, что его аппаратом заинтересуются технологические компании, но хотя аппарат не был коммерческим, в него сыграли более ста тысяч человек, 90% из которых не смогли обыграть компьютер. Так как Эдвард никак не монетизировал свое изобретение, а предложений о сотрудничестве он не получил – его идея стала финансовым провалом компании Westinghouse Electric, а дальнейшее развитие стало невозможным. Несмотря на финансовую несостоятельность Nimatron стал отправной точкой в игровой индустрии. Этот автомат не имел никаких потребностей в обеспечении безопасности.

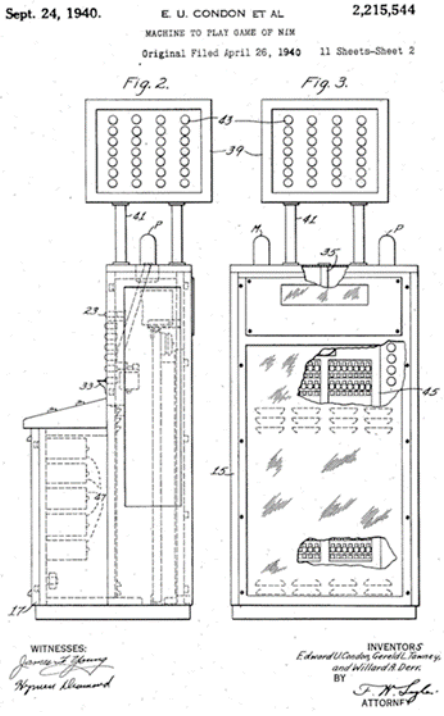
Sept. 24, 1940. E. U. CONDON ET AL. 2,215,544
MACHINE TO PLAY GAME OF NIM
Original Filed April 26, 1940 11 Sheets-Sheet 2
Fig. 2. Fig. 3.
WITNESSES:
INVENTORS
ATTORNEY

Рис. 1. Схема игрового автомата Nimatron

В последующие 20 лет хоть и создавались прототипы таких игровых автоматов как крестики-нолики, теннис, шахматы, но они были невероятно дорогими, громоздкими и чаще всего существовали в одном экземпляре в университетах, где и были созданы. Основное развитие технологий видеоигр произошло благодаря государственным заказам на обучающие симуляторы для военных.

После массового распространения компьютеров IBM серии 700, которые стали революционными в начале 1960-х годов, множество программистов стали пробовать свои силы в создании простых игр на этой платформе. Игра spacewar (рис. 2), созданная Стивом Расселом стала настоящим прорывом в игровой индустрии, так как была увлекательной и простой в освоении. Игра была примитивной в своей графике и механиках, но увлекательность процесса вместе с ощущением того, что ты участвуешь в космической битве, вызывала фурор у пользователей. Никаких систем защиты эта игра не имела, поэтому она очень быстро распространилась на множество других компьютеров серии IBM 700. Стив Рассел не патентовал свою разработку и в результате не получил со своей игры никаких дивидендов. Популярность spacewar и других игр показала, что видеоигры должны иметь защиту от взлома и копирования, так как могут пользоваться большой популярностью, несмотря на маленький процент населения, у которого на тот момент был доступ к компьютерам IBM 700.

Рис. 2. Spacewar на компьютере PDP-1

Это дало толчок к развитию аркадных автоматов. Несмотря на дороговизну производства, их начали выпускать крупнейшие компании развлекательной индустрии, начиная с конца 1960-х годов, так как увидели возможность для освоения нового рынка. Первые

аркадные автоматы приносили большие убытки, но компании стремились осваивать технологии раньше остальных, чтобы первыми закрепиться в новой отрасли. Многие компании позже полностью переключились на производство видеоигр: такие компании, как Konami, Nintendo и Namco (в данный момент Bandai Namco) до сих пор являются крупными представителями видеоигровой индустрии. У первых аркадных автоматов также была цель приобщить общество к новому виду развлечений, ведь стоимость за одну игру едва покрывала затраты на электроэнергию и износ деталей. Основой для первых аркадных автоматов служили слот-машины из казино (также из-за того, что первые производители аркадных автоматов занимались в том числе производством слот-машин для залов азартных игр), как следствие – все системы защиты казино-автоматов сводились к особому строению корпуса и системы вброса монет с защитой от взлома, в том числе «монет на верёвочках». Эти аркадные автоматы были изолированными от любых вмешательств, потому что каждый автомат имел специализированное аппаратное обеспечение, которое было невозможно или чрезвычайно трудоёмко модифицировать на любых компьютерах того времени. Единственной возможностью несанкционированного доступа была кража самих автоматов, что было крайне затруднительно, учитывая их габариты. Так появились первые системы обеспечения безопасности в видеоиграх. Замкнутость таких систем делала нецелесообразными все попытки взлома и несанкционированного доступа.

В то же время стали выпускаться более универсальные персональные игровые системы. В 1972 году появилась домашняя приставка Magnavox Odyssey, с которой началось первое поколение игровых приставок. Она работала на диодно-транзисторной логике с использованием диодов и дискретных транзисторов. Такая приставка могла выводить на экран три квадратных точки и вертикальную линию, двумя точками можно было управлять с помощью контроллеров, а третья управлялась системой. С играми шли полупрозрачные пленки с цветными пластиковыми накладками на экран телевизора, и со сменой игрового картриджа необходимо было менять эту пленку. Данная приставка была скорее рекламой самих телевизоров компании Magnavox (подразделение компании Philips), чем полноценным коммерческим продуктом, поэтому все доступные игры шли сразу с приставкой. Из-за этого потребности в обеспечении безопасности попросту не было. Сами же картриджи представляли собой перемычки между разными контактами, запускающими одну из игр, которые уже были в Magnavox Odyssey.

В этом же году вышел легендарный аркадный автомат PONG (рис. 3), который стал первым коммерчески успешным игровым автоматом. Высокая популярность стала причиной его портирования на домашние игровые приставки и привела к бурному развитию домашних игровых приставок. Приставка PONG имела всего одну игру и была уменьшенной версией аркадного автомата. Все приставки первого поколения были узкоспециализированы и дороги в производстве. Они не имели никаких причин для взлома, и по причине своей «узконаправленности» стали довольно быстро уходить с рынка. Единственной распространенной возможностью несанкционированного доступа была модификация схем сломанных приставок, так как вскрывать рабочую приставку было попросту нецелесообразно. Но таких модификаций было настолько мало, что никакого значительного финансового вреда они не наносили, поэтому производители не обращали на это внимания.

Рис. 3. Аркадный автомат PONG

В 1976 году началось второе поколение домашних приставок, начавшееся с выходом первой микропроцессорной приставки Fairchild VES. В новых системах устройство уже было восьмиразрядным компьютером. И если примитивные картриджи первого поколения были набором соединений между контактами самой приставки, то второе поколе-

ние перешло на сменяемые микрочипы, которые кодировались с помощью дискретной логики. Так называемые «восьмибитные» системы позволили расширить возможности в разы, так как у новых приставок появилась полноценная графика и даже своя звуковая система. И за то, и за другое отвечал отдельный телевизионный чип, встроенный в архитектуру. Со второго поколения приставок началось активное развитие несанкционированного взлома видеоигр, которое в основном было завязано на копировании микросхем. По современным меркам строение картриджей выглядело примитивным. Главным элементом был микрочип, подделка которого стала главной задачей пиратских объединений, впервые появившихся именно в это время. Несанкционированное производство картриджей позволило пользователям гораздо дешевле опробовать новинки игрового рынка.

Рис. 4. Игровая приставка Atari 2600 и процессор MOS Technology 6507

Впервые в истории игровое пиратство существенно повлияло на прибыль официального производителя. Больше всего пострадала приставка Atari 2600, которая была лидирующей на рынке. В качестве процессора использовался MOS Technology 6507 (рис. 4) с частотой 1.19 МГц, который был урезанной версией MOS Technology 6502, стоявших на персональных компьютерах Apple I и Apple II. Оперативной памяти было всего 128 байт, в которую включался и стек вызовов, и полное состояние игрового мира. Примечательно, что в данной системе попросту не хватало памяти для экранного буфера, который бы загружал кадр перед отправкой его на экран. Буфер сохранял только пиксель последующего положения луча на экране, при этом после прохождения последней активной строки был кадровый гасящий импульс. В этот промежуток игра обрабатывала входные данные для обновления информации о том, что должно было появиться на экране. И если в тайминге при этом возникала ошибка, то на экране появлялись множественные артефакты, которые назвали «гонка за лучом».

Для удешевления самой консоли был выбран самый недорогой интерфейс картриджей. Он имел 12 адресных линий, благодаря чему использовалось только 4 Кб памяти картриджа. Это делало невозможным создать программную защиту, но компания Atari и не рассчитывала на то, что будут выпускаться нелицензионные картриджи, так как массовых инцидентов до этого не было. На волне успеха даже крупные компании стали делать свои видеоигры на эту систему, так как отношение к игровой приставке было как к обычному проигрывателю. Если компания выпускает DVD-диски, она не обязана платить отчисления всем DVD-проигрывателям, которые могут запустить их диск. Такие отношения к лицензиям на Atari 2600 привели к большим убыткам и множеству судебных разбирательств, а рынок видеоигр был переполнен настолько плохими по качеству игр, что доверие к Atari 2600 стало стремительно падать. Более того, злоумышленники создали клон данной приставки со встроенной внутренней памятью, в которой уже было заложено несколько десятков игр. Atari 2600 продавалась в США, Франции, Германии и Японии, а клон RAMBO распространялся во всем остальном мире. На упаковке этой приставки был актер Сильвестр Сталлоне в образе персонажа из одноименного фильма Рэмбо, которого также разместили незаконно. Поэтому на последующих приставках этого поколения, таких как Emerson Arcadia 2001, Vectrex и ColecoVision была сделана особая форма картриджа и слота под него, которую сложно воспроизвести без особого оборудования, хотя и это вряд ли спасло их от подделки. Малая популярность других приставок по срав-

нению с Atari 2600 свела на нет попытки последующего взлома этого поколения приставок.

В 1983 году после кризиса игровой индустрии стали выходить игровые устройства третьего поколения. Восьмиразрядные игровые системы ознаменовали новую эпоху видеоигр, когда они стали очень массовым явлением в обществе. В этом же году появляется понятие «платформодержатель», означающее, что производители программного обеспечения для специализированных платформ должны соблюдать лицензионные условия и быть юридически оформлены с компанией, выпускающей систему для легального выпуска своей продукции. Самыми знаковыми игровыми системами в этом поколении были японские приставки Famicom и Sega Master System, которых было продано суммарно более восьмидесяти миллионов экземпляров. Такая большая популярность привела к огромному развитию нелицензированных копий. Нарушение авторских прав в видеоигровой индустрии достигло своего пика именно в третьем поколении. Были целые официально-оформленные компании, которые в огромных масштабах выпускали копии, как картриджей, так и целых приставок. Более того, многие разработчики сами создавали и продавали нелицензированные игры, чтобы не отчислять процент от продаж компаниям Sega и Nintendo. Началось настоящее противостояние систем защиты и взлома.

Famicom (сокращение от Family Computer), выпускавшаяся в Северной Америке и Европе под названием Nintendo Entertainment System (NES) была лидирующей на рынке (рис. 5) и имела выдающиеся технические характеристики. В особенности, систему выделял восьмибитный процессор Ricoh, также совмещающий в одном кристалле звуковой процессор и контроллер DMA, ещё сильнее выделялся видеоконтроллер Ricoh, поддерживающий сорок восемь цветов и «спрайты» на аппаратном уровне.

Рис. 5. Версия NES для Северной Америки

Встроенная комплексная lock-out аппаратная система защиты 10NES состояла из двух частей комплекса Checking Integrated Circuit (CIC). И чип блокировки внутри NES, и чип на картридже являлись частями одной схемы (рис. 6). Чип внутри NES, действовал как замок, а чип в картридже – как ключ. Разница была лишь в том, как они подключены. Система составлена таким образом, что выход одного CIC подключен к входу другого, и наоборот. Замок и ключ повышают напряжение до +5 В внутри NES и заземляются на картридже. Оба имеют одни и те же тактовые импульсы 4 МГц, передавая их на контакт 6. Контакт RESET на ключе подключен к SLAVE CIC RESET на замке. Вывод RESET замка подключен к шине сброса системы. Это можно продемонстрировать, вставив игру в приставку с уже включенной системой. NES не будет работать, пока не будет нажата кнопка Reset, сбросив блокировку CIC, которая в свою очередь сбрасывает ключ. CPU & PPU RESET не подключен на ключе, а на замке он подключен к контактам сброса CPU и PPU. Контакты 11 – 15 заземлены на оба CIC в NES; они фактически используются в многопользовательских системах, так что в одной системе могут быть адресованы несколько CIC. Таким образом, вся цепь переходит на + 5 В и запускает игру.

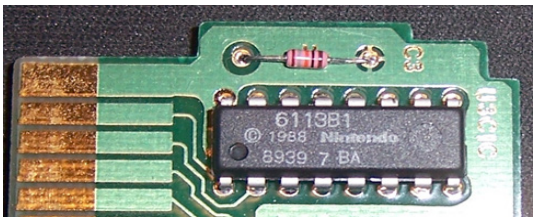

Рис. 6. Чип безопасности 10NES для Famicom

Как только система выходит из режима загрузки, замок посылает соответствующие сигналы сброса и инициализации на ключ. Затем ключ должен вернуть правильный ответ, в противном случае блокировка будет удерживать CPU & PPU RESET в режиме ожидания с импульсами прямоугольной волны частоты 1 Гц. После прохождения проверки замок может сбросить ключ, оба CIC синхронизируются друг с другом, а система запускается.

Комплекс состоит из четырехбитного микроконтроллера SM590, находящегося в са-

мой приставке, который проверял вставленный картридж на предмет аутентификации. Если ключ не проходил проверку, то Famicom просто перезагружалась до тех пор, пока чип не пройдет проверку. Такая система стала довольно эффективной и обеспечивала не только предотвращение запуска нелицензированного программного обеспечения, но и полный контроль над выпускаемой продукцией, включая возможность региональной блокировки игр, не предназначенных для выхода в определенных странах. Региональная блокировка никак не считывала геопозицию, поэтому для разных стран выпускали разные версии Famicom, которые отличались в том числе и региональными данными в микроконтроллере. Производители нелицензионной продукции из-за невозможности создать чипы с подходящими ключами стали обходить систему безопасности как на уровне выше, так и на уровне ниже этого чипа. В картриджи стали встраивать системы подключения через оригинальный картридж, таким образом владелец NES мог подключить пиратский картридж к любому лицензионному, и система защиты распознавала чип именно с лицензионного, но запускала при этом нелицензированный. Помимо этого, появилось множество аппаратных клонов самой приставки. Они имели множество модификаций печатных плат с интегральными схемами, объединенными чипами и другими методами удешевления производства. Как и в случае с Atari 2600 клоны приставки были распространены в тех странах, где Famicom официально не выпускалась. Более того, почти в каждой стране от стран СНГ и Южной Америки до Южной Африки и даже Северной Кореи были свои аппаратные клоны NES. В одной только России «скопированной» приставки Dendy было продано более двух миллионов экземпляров. Общество того времени настолько не привыкло к лицензированию, что отдельные магазины для клонов, реклама по телевизору и даже отдельные телепередачи, посвященные этим приставкам, были абсолютно нормальным явлением, тем более, что аппаратные клоны не имели системы защиты и запускали любые картриджи. По неофициальным данным количество аппаратных клонов было примерно равно количеству проданных приставок Famicom. Несмотря на это, финансовые потери компании из-за пиратства были довольно малы, так как нелицензионных картриджей было довольно мало, а клоны в основном продавались в странах, где Nintendo Entertainment System никогда официально не выпускались.

Остальные приставки третьего поколения, включая Sega Master System и Atari 7800 имели очень схожую архитектуру и системы защиты. А в силу подавляющей популярности Famicom практически не подвергались несанкционированному взлому.

Четвертое поколение игровых приставок появилось в 1987 году с выпуском PC EngineTurboGrafx-16 от компании NEC, которая стала первой шестнадцатиразрядной игровой системой. Популярностью данная игра не пользовалась, поэтому новое поколение вышло в массы в 1988 – 1990 годах с выходом приставок Super Nintendo Entertainment System и Sega Mega Drive (рис. 7). В это же самое время появились портативные игровые консоли, такие как Nintendo Gameboy, Sega Game Gear и Atari Links. Игры окончательно перестали быть нишевым продуктом, одними только портативными Gameboy в поездках и перелётах пользовались многие публичные люди, такие как группа Metallica, актёр Робин Уильямс, политик Хиллари Клинтон и множество других. В домашних приставках этого поколения системы защиты немного изменились. Рассмотрим системы защиты в двух основных системах этого поколения.

Рис. 7. Японская версия Sega Mega Drive

Sega Mega Drive уже имела в своем составе 16/32-разрядный процессор Motorolla 680000 и дополнительный 8-битный процессор Zilog Z80, отвечающий за управление звуковыми устройствами. 72 Кб оперативной памяти и 64 Кб видеопамяти значительно расширили возможности консоли. Она уже могла отображать на экране 64 цвета из палитры в 512-оттенков. Для обеспечения безопасности система использовала встроенную в материнскую плату TradeMark Security System. Использовался двухбитный чип, который имел две стадии проверки. При запуске игры

TradeMark Security System проверяет память ПЗУ картриджа по адресу $100, есть ли по этому адресу слово «SEGA» в кодировке ASCII. За этот шаг отвечала программная часть системы защиты, и после прохождения этой части на экран выводилось сообщение «Produced By License From Sega Enterprises Ltd.». Система проверки держалась в строгой секретности, что сработало очень хорошо, так как взломать эту систему удалось только после основного периода продаж приставки. Далее шла уже привычная система проверки с помощью контроллера ввода-вывода, который ограничивал доступ к порту данных VDP, если в чипе картриджа не содержалось слова «SEGA» по адресу $A14000. Новые картриджи имели структуру, которая не позволяла подключить через них нелицензионный картридж для обхода второй стадии, но они появились намного позже из-за утечек информации от официального издателя Absolute Entertainment и не сильно повлияли на прибыль компании Sega.

Приставка Super Nintendo Entertainment System (SNES) в свою очередь использует незначительно модифицированную Checking Integrated Circuit, а форма картриджей также была изменена таким образом, чтобы подключить через них нелицензированный картридж было практически невозможно, не испортив оригинальный картридж. Но в это же время появилось такое понятие как «прошивка» игровой приставки, которая заключалась в удалении чипа проверки безопасности и запаивания контактов на месте этого чипа. Этот способ позволял запускать на ней любое нелицензированное программное обеспечение, что сильно развязало руки производителям пиратских копий видеоигр.

Примечательно, что именно в этом поколении появились в продаже отдельные подключаемые устройства, читающие компакт-диски, так как очень малого объема памяти картриджей явно не хватало для реализации новых амбиций видеоигровых разработчиков.

Пятое поколение берет свое начало в 1993 году. После очередного кризиса игровой индустрии произошел невероятный рост как количества компаний, выпускающих свои платформы, так и количества видеоигровых студий. Игры совершили огромный скачок, потому что появилась трехмерная графика, возможности расширились в сотни раз за счет использования компакт-дисков, которые вмещали куда больше памяти и были более износостойкими, а увеличенные мощности позволили создать полноценную операционную систему в игровых приставках.

В тот момент игровая индустрия разрослась настолько, что рассмотреть системы защиты всех игровых консолей и самих игр в рамках этой работы попросту невозможно, поэтому рассмотрим только игровую консоль Sony PlayStation (рис. 8) и Персональный Компьютер, которые были двумя самыми популярными игровыми системами во время пятого поколения игровых приставок.

Рис. 8. Sony Playstation

Сначала рассмотрим средства защиты на консоли PlayStation, которой было продано более ста миллионов экземпляров. Sony PlayStation имела центральный процессор MIPS R3000A и 32-разрядный RISC-микропроцессор, работающий на частоте 33,9 МГц с производительностью в 30 MIPS. Чип содержал контроллер для работы с трехмерной графикой (Geometry Transformation Engine) с производительностью в 66 MIPS, который находился на одном кристалле с центральным процессором. Память основного ОЗУ была 2 Мб, видео ОЗУ – 1 Мб, а звукового ОЗУ – 512 Кб. У этой приставки была региональная блокировка, подобная тем, которые рассматривались ранее. Данная блокировка, как и раньше, одновременно служила для проверки лицензии диска. Лицензионные игры PlayStation имели отмеченную зону в крайней области диска, которая содержала информацию о регионе, эта информация состояла из букв SCEx, где x – область диска: A – для Америки (SCEA); E – для Европы (SCEE); Я – для Японии (SCEI); W – для тестирования разработчиками (SCEW).

В случае если консоль определенного региона не обнаружит в своей области нужной кодировки, то система не запустится. Нелицензионные диски не имеют такой метки, так как обычные дисководы не могут прочитать эту часть диска, поэтому система также откажется загружать игру.

Как и в Sega Mega Drive текст на экране «Лицензировано Sony Computer Entertainment America SCEA TM» находится не в самой системе, а на диске в области проверки лицензионности. Система читает этот текст с диска и помещает его в логотип загрузки, что позволило делать каждой игре собственные загрузочные экраны.

Злоумышленники использовали два способа обойти эти ограничения. Первый – с помощью специального диска Import Player. На этом диске использовался «эксплойт», который представляет собой использование способности системы играть в многодисковые игры. Некоторые игры не помещались на один носитель и в какой-то момент выводили сообщение о необходимости сменить игровой диск. Когда пользователь меняет диски, система не выходит в режим загрузки, поэтому вторая проверка вставленного диска не выполняется. Но происходит первичное считывание, которое решает модифицированный чип безопасности. Модификация чипа была схожа с «прошивкой» Super Nintendo Entertainment System с единственным отличием, что чип не вынимался с запаиванием контакта, а к нему припаивался элемент, имитирующий региональный код, и благодаря этому региональную блокировку была возможность обойти. Второй метод был гораздо более надежный, но схожий с добавлением пользовательской загрузки, только в этом случае правильный загрузочный текст был введен в компакт-диск, что позволяло загружать его напрямую.

Другая мера, которая была реализована – обнаружение модифицированных чипов. Она потребовала внедрения нового аппаратного обеспечения, поэтому она была доступна только в более поздних версиях устройства. Кроме того, это мера исполнялась не кодом системы, а кодом игры, поэтому код должен был быть внедрен в саму видеоигру, то есть компакт-диски старых ревизий не могли использовать данную функцию.

Обнаружение модифицированного чипа происходит следующим образом: обычный чип проверяет региональный код компакт-диска (SCEx, как мы видели выше), но новые диски также в ответ проверяют успешность региональной проверки, поэтому если в системе есть модифицированный чип, то официальные игры просто не будут на ней запускаться.

Обойти эту защиту можно было с помощью еще одного внедряемого чипа (у которого есть патч для обнаружения «антимодчипа») или путем исправления кода игры перед нелицензионной записью. Эти способы уже были куда менее популярны, так как были очень трудозатратны.

Несмотря на то, что у этой игровой консоли уже были модули подключения к интернету, закрытость системы и провальные попытки взлома не дают возможности узнать о системах интернет-защиты на этой приставке.

Если обратить внимание на игровой рынок персональных компьютеров, то системы взлома были куда более разнообразны из-за большей открытости операционной системы, а отсутствие специализированной системы, такой как игровая консоль попросту не давали играм централизованной защиты. Так как в это время даже не было специализированного программного обеспечения по защите видеоигр, каждая игровая студия была вынуждена самостоятельно создавать программное обеспечение для защиты своей игры от взлома.

Игровое пиратство и несанкционированный доступ к данным в компьютерных играх девяностых годов были настоящей катастрофой, масштабы которой удалось оценить только спустя несколько лет. Тот факт, что пиратских копий было в разы больше лицензионных дисков, стал наименьшей проблемой безопасности, например, в России официальными были всего пять процентов от всех продаваемых компьютерных видеоигр. Но если огромное количество уязвимостей в однопользовательских играх вело к их взлому для незаконного распространения копий, то взлом аккаунтов набирающих популярность онлайн-игр вел к несанкционированному доступу к персональным данным пользователей, банковским реквизитам и даже контролю над компьютерами пользователей. Из-за слабого развития интернет-культуры и онлайн-гейминга в период с 1990 до 2000 года были похищены данные более чем трех миллионов пользователей по всему миру с помощью фишиноговых сайтов, взлома игровых серверов с данными и использования уязвимостей игрового кода. С такими последствиями сталкивались онлайн-игры всех размеров и жанров, ведь даже такие «мастодонты онлайна» как Ultima Online, Lineage, Neverwinter Nights и The Realm Online испытали на себе многочисленные взломы через использование найденных уязвимостей. В последующее

время шло развитие, как аппаратных средств защиты, так и программных. Но аппаратные средства, по сути, являлись улучшенными модификациями старых версий, а разбирать все этапы улучшения программной защиты было бы просто нецелесообразно в рамках одной статьи по причине большого объема информации, поэтому далее рассмотрим современные средства защиты видеоигр.

В настоящее время все видеоигровые платформы содержат куда больше информации о пользователе, чем когда бы то ни было. Это могут быть данные банковских карт, электронная почта, адрес проживания и даже паспортные данные (как например в Китае). В Российском законодательстве видеоигры должны рассматриваться как информационные системы персональных данных (ИСПДн) и никак не отделяются. В мировой практике практически нет специализированных нормативных документов, регулирующих видеоигры. Но такие документы как общий регламент по защите данных (GDPR), действующий на территории Европейского Союза, были отредактированы с учётом того, что под их регламент попадают видеоигры. При этом данный регламент покрывает требования к ИСПДн большинства стран, поэтому чаще всего игровые студии опираются именно на него.

В данный момент игры имеют куда больше средств защиты, чем раньше, так как основную часть обеспечения безопасности берут на себя компании, производящие игровые консоли и компании-владельцы игровых «лаунчеров», которые представляют собой агрегатор по продаже и запуску видеоигр. Для персональных компьютеров их довольно много: Steam, Epic Games Store, UPlay (рис. 9) и множество других, в то время как на мобильных платформах такие «лаунчеры» создаются самими разработчиками операционных систем, такими как Apple и Google.

Рассмотрим систему защиты «лаунчера» Google Play Market. Система Android имеет средство защиты Google Play Protect, которая сканирует каждое приложение, попадающее в Play Market. Эта система для улучшения функционала использует машинное обучение. Она проверяет все пакеты данных приложения, все файлы и все данные. Не смотря на то, что эта система является одной из передовых, она имеет большое количество уязвимостей и не позволяет разработчикам узнать об этих уязвимостях из документаций. Система работает как на уровне принятия приложения в свой магазин, так и на уровне сканирования данных, используемых пользователем.

Рис. 9. Крупнейшие современные лаунчеры

В основе большинства систем защиты, таких как StarForce, которая является одним из крупнейших российских представителей в обеспечении безопасности в видеоиграх, используется преобразование кода в .Net код виртуальной машины, шифрование строк и массивов, преобразование кода в цифровую форму, введение ложных связей, объединение участков кода и другие. Многие системы защиты используют собственный язык программирования для усложнения взлома. В процессе защиты исполняемый файл разбирается на составные части. Составные части исполняемого файла преобразуются с использованием различных технологий защиты. Помимо этого, существует множество методов защищенной «контейнеризации» данных, методов проверки целостности и внешней привязки видеоигры. Из этих инструментов чаще всего и выстраивается комплексная защита. В силу специфики видеоигр, системы защиты, не встроенные в игровую среду разработки или платформу, не могут быть универсальными и вынуждены подстраиваться под каждый проект.

Несмотря на кажущуюся полноценную безопасность, инциденты, связанные с современными игровыми системами, не исчезают. Постоянно находятся новые уязвимости, порождающие новые преступления с хищениями денежных средств, пользовательских данных и целых аккаунтов.

На данный момент одним из наиболее популярных методов взлома является метод reverse engineering, при котором злоумышленник с помощью декомпиляторов «разбирает» код игры для поиска мест потенциальных уязвимостей. После нахождения таких мест нарушитель запускает ботов, которые

проверяют каждое место на непосредственное наличие уязвимостей. Далее создаются уже специализированные боты, которые проверяют каждую найденную уязвимость и используют её. Также зачастую используют запуск видеоигры на виртуальной машине для просмотра кода операционной системы во время работы видеоигры.

Представленное исследование систем защиты в видеоиграх подчеркнуло комплексность развития всех систем и стратегий действий злоумышленников и противодействия им. Возможности систем нарушителей растут, поэтому для правильного выстраивания стратегии обеспечения безопасности необходимо изучать предыдущие системы и опыт их развития. Потому как в современных продуктах игровой индустрии выяснить реализованные меры практически невозможно из-за того, что системы являются конфиденциальными для поддержания требуемого уровня сохранности данных.

Таким образом, инструменты защиты платформодержателей и разработчиков постоянно совершенствуются для обеспечения приемлемого уровня сохранности информации. Быстрое реагирование на инциденты со стороны видеоигровых разработчиков и соблюдение простых мер информационной безопасности со стороны игроков уменьшает шанс несанкционированного доступа к данным пользователя.

Литература

1. Стивен Л. Кент «The Ultimate History of Video Games» - Three Rivers Press : 2001 – С. 10–624 с.
2. Blake J. Harris «Console Wars» : 2014 – С. 7–244 с.
3. Peter Leigh «The Nostalgia Nerd's Retro Tech: Computer, Consoles & Games.» : 2018 – С. 5–186.
4. Brian J. Wardyga «The Video Games Textbook: History • Business • Technology» : 2018 – С. 6–252.
5. Тристан Донован, Ричард Гэрриот «Replay: The History of Video Games» : 2010 – С. 8–373.
6. Bill Loguidice, Matt Barton "Vintage Game Consoles: An Inside Look at Apple, Atari, Commodore, Nintendo, and the Greatest Gaming Platforms of All Time" : 2014 – С. 5–315.
7. Andy Bossom, Ben Dunning - "Video Games: An Introduction to the Industry" : 2015 – С. 23–30.

References

1. Steven L. Kent «The Ultimate History of Video Games» - Three Rivers Press : 2001 – S. 10–624.
2. Blake J. Harris «Console Wars» : 2014 – S. 7–244 с.
3. Peter Leigh «The Nostalgia Nerd's Retro Tech: Computer, Consoles & Games.» : 2018 – S. 5–186.
4. Brian J. Wardyga «The Video Games Textbook: History • Business • Technology» : 2018 – S. 6–252.
5. Tristan Donovan, Richard Garriott «Replay: The History of Video Games» : 2010 – S. 8–373.
6. Bill Loguidice, Matt Barton "Vintage Game Consoles: An Inside Look at Apple, Atari, Commodore, Nintendo, and the Greatest Gaming Platforms of All Time" : 2014 – S. 5–315.
7. Andy Bossom, Ben Dunning - "Video Games: An Introduction to the Industry" : 2015 – S. 23–30.

АНФИНОГЕНОВ Максим Викторович, студент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080 Челябинск, проспект Ленина, 76. E-mail: anfinogenov.max1997@yandex.ru.

АНТЯСОВ Иван Сергеевич, старший преподаватель кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080 Челябинск, проспект Ленина, 76. E-mail: antiasovis@susu.ru.

ANFINOGENOV Maksim Viktorovich, Student of Department of Information Security, South Ural State University (National Research University). 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: anfinogenov.max1997@yandex.ru.

ANTYASOV Ivan Sergeevich, Senior Lecturer of Department of Information Security, South Ural State University (National Research University). 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: antiasovis@susu.ru.