

# Instant Netrunning

## A Fuzion Plug-In

by Christian Conkle

(conkle@europa.com, <http://www.europa.com/~conkle>)

Перевод Lex Rem ([lexrem@mail.ru](mailto:lexrem@mail.ru))

<http://lexrem.narod.ru>

### Вступление

Это - расширение для правил взлома и хакинга в системе Fuzion и Interlock. Эти правила основаны на правилах Netrunning для Киберпанка, и предназначены, в основном, для миров киберпанка где используются нейро-киберинтерфейсы. Хотя они достаточно хорошо могут подойти и для современного или фантастического мира.

Эти правила были разработаны, чтобы использовать существующее оборудование и программное обеспечение Киберпанка 2020 с небольшими модификациями. Есть несколько отличий от первоначальных правил, которые предназначены, чтобы ускорить и упростить игру.

Во-первых, эти правила упрощают сеть. Движение в пределах виртуальной среды киберпространства концептуально. Для преобразования приложений, использующих "диапазоны", просто применяется шанс процента эффективности, основанный на диапазоне.

Во-вторых, эти правила используют атрибут Мощность (Power) из других Fuzion игр, по существу эквивалент компьютерного интеллекта из CP2020. В-третьих, программное обеспечение и память больше не должны быть назначены на определенный CPU. По желанию ДМа, каждый МУ приложения или файла данных может быть назначены на определенный CPU так, что если CPU терпит неудачу, приложение или файл данных больше не доступны.

Этот процесс был удален, чтобы устранить дополнительные расчеты. Эти правила используют механику 3d6 броска. Если Вы играете с использованием Interlock или опциональный 1d10 Fuzion, просто замените бросок 3d6 на 1d10. Вы не достигните того же самого вида кривой распределения бросков, но результаты будут более случайны.

### Сеть

Сеть - глобальная компьютерная сеть, позволяющая быстрый и удобный доступ на миллионы компьютеров из любого другого компьютера на земле или в космосе. Любой компьютер, связанный с этой сетью имеет возможность доступа к информации из любого другого компьютера, связанного с этой сетью, независимо от расстояния или времени дня. Называется ли это Интернетом, Сеткой, Киберпространством, Паутиной или Галанетом, все они используют различные специальными эффектами и технологии, чтобы делать одно и то же. Это расширение использует мир ближайшего будущего, где используется интерфейс Виртуальной Реальности и дает общие названия действиям и задачам, которые могут быть легко изменены, чтобы больше соответствовать другим сеттингам.

Всем компьютерам, связанным с Сетью назначены LDL. Этот LDL служит как своего рода номер телефона для этого Компьютера, с помощью которого другие компьютеры знают, куда послать информацию. В футуристическом сеттинге, это может быть виртуальный адрес или образ (неважно, как это назвать). Пользователь Сети подключает свой компьютер к Интерфейсу Виртуального Мира, в пределах которого Компании оплачивают место и создают сложную виртуальную конструкцию, чтобы представить свой LDL. (VR эквивалент Интернет порталов типа Infoseek или Yahoo! в настоящем времени). Пользователь теперь может путешествовать по шумному 3-D Виртуальному Городу, независимо от гравитации или скорости. Корпоративные виртуальные конструкции подобны гигантским трехмерным рекламным плакатам, которые пытаются заманить простого пользователя в их VR, чтобы продать изделия или услуги. Некоторые VR, фактически предоставляют полезные услуги типа информационных услуг или онлайн-приложений. VR - эквивалентны современным Вебсайтам. Эти VR (в дальнейшем Виртуалы) размещены на серверах данных, обслуживающихся соответствующими корпорациями или

учреждениями. И есть информация, размещенная на этих серверах и недоступная простым пользователям, которая притягивает Хакеров.. Обычно, корпоративный сервер открыт для доступа публики сети, обеспечивая информацию как для общественности, так и для служащих через разнообразие интерфейсов: текст, текст и графика (Паутина), звук/видео или полносенсорный Виртуальный мир (Сеть).

Однако, ценность общедоступной информации на публичных серверах невелика и малозначима. Кроме того, доступ к сетевому программному обеспечению ограничен приложениями общественной области.

Защищенные Сервера или Инфофорты (Datafortresses) - ограниченные скрытые уровни сервера, обеспечивающие удаленный доступ к данным или приложениям с ограниченным доступом для уполномоченных пользователей. Безопасность поддерживается через брэндмауер (DataWall) сервера.

Уровень ограничения безопасности зависит от ценности информации или приложения. Секретная информация может быть размещена на том же самом сервере, что и общественная информация, только скрыта в защищенных директориях, невидимых для пользователей, которые не имеют надлежащих прав доступа. Авторизация происходит с помощью надлежащей процедуры идентификации.

Идентификация может принимать множество форм: Авторизированная Сеть LDL, пароли, особое программное обеспечение, или даже Биометрические данные.

Цель хакера в жизни - получить неограниченный доступ к ограниченной информации, раскрывать тайны, делать неправомерные изменения в данных, или использовать закрытое программное обеспечение.

При попытке получить неавторизованный доступ к корпоративному серверу, хакер устанавливает легальный контакт с сервером компании. После установки связи, хакер получает обычный доступ к свободным услугам.

Обычно, после этого, неавторизованный пользователь использует программу интерфейса, чтобы получить доступ к закрытым данным сервера. Программа авторизации или Гейт (Code Gate) проверяет идентификацию и позволяет доступ. Хакер делает попытку обмануть Гейт. Если это не удастся, хакер может попытаться получить вход, выведя из строя брэндмауер, защищающий информацию.

Но даже после входа, сервер постоянно перепроверяет авторизацию с помощью сканирующего программного обеспечения (Detection software). Сканер постоянно перепроверяет всех пользователей, связанных с сервером. Если он находит несоответствие или ошибку, он уведомляет Сисадмина, который попытается отключить хакера, определить его местоположение с помощью трейсера, повредить его программное обеспечение с помощью Айс, разрушить компьютер хакера с помощью Антисистемы (Anti-System), или физически повредить Хакера с помощью программ Антиперсонал. Хакер использует программы Стелс для обмана Сканеров, заставляя их либо принимать либо игнорировать соединение хакера. При обнаружении, хакер может сопротивляться действиям Сисадмина с Айсом и др. с помощью своих программ.

Если хакер получает доступ к данным инфофорта, он может изучать, копировать, или изменять данные. Данные имеют вид диалоговых приложений для удаленного использования, межофисных коммуникаций, публичных форматов данных (текст, звук, видео или VR), баз данных или отчетов.

## **Хакер**

Арсенал Хакера включает компьютер, специализированное программное обеспечение и способ соединиться с отдаленным компьютером, обычно через Сеть, с помощью прямого соединения.

Доступ в Сеть для хакера очень важен. Чтобы соединиться с Сетью, Хакер должен иметь LDL. Стоимость LDL - 50\$ в месяц от Интернет Корпорации, хотя они также могут быть хакнуты.

Связь между компьютерами относительно легко проследить. Каждое компьютерное соединение имеет соответствующий Уровень Отслеживания от 1 до 10. Обычно, хакеры делают цепь из нескольких соединений, прежде чем соединяются с нужным компьютером. СисАдмин, желающий отследить Хакера, должен проследить каждое соединение, чтобы найти источник.

### **СисАдмин**

СисАдмин отвечает за безопасность сервера. Их главная задача – предотвратить незаконное получение хакером неправомерного доступа к ограниченным данным. Их вторичная задача - поймать хакеров, которые уже имеют доступ. Сисадмины используют свои собственные компьютеры, связанные с сервером, чтобы запустить приложения.

Сам сервер использует программное обеспечение типа Гейтов, Файрволов и Сканеров, чтобы удерживать и идентифицировать хакеров и в то же время позволить легальным пользователям получить доступ к информации.

Сервер также характеризуется своей Мощностью и Скоростью. Также он оценивается Уровнем Безопасности от 1 до 10. Это число добавляется подобно навыку к мощности компьютера при выполнении приложения. Уровень Безопасности компьютера также является его Уровнем Отслеживания, если он используется в цепи соединений.

СисАдмин не может сделать что-либо для поимки Хакера, если он не знает, что он здесь, так что СисАдмин в основном сильно полагается на Сканирующие программы, которые могут уведомить о попытке неправомерного доступа. После обнаружения, СисАдмин может запустить программы АнтиПерсонал против вторгшегося, или решить выследить хакера и запустить программы Антисистема против компьютера Хакера.

### **Компьютеры**

Компьютеры, являются ли они Пальмтопами, Десктопами, Ноутбуками или Майнфреймами, необходимы для выполнения программ. Компьютер характеризуется Мощностью, Скоростью и Уровнем Безопасности.

Мощность используется подобно характеристики BODY и REF компьютера, показывает его стойкость к атакам и его основной шанс на выполнение действий. Мощность основана на количестве процессоров (CPU), которыми оснащен компьютер. Один CPU имеет Мощность 3, каждый дополнительный CPU добавляет еще 3. Каждый CPU стоит 10,000 \$. Компьютер может иметь до 7 CPU до мощности = 21. Дополнительное увеличение количества CPU, улучшает обрабатывающую способность и обеспечивает резерв на случай, если один из CPU выйдет из строя в результате работы программ комплекса Антисистемы.

CPU Компьютера также определяет количество программного обеспечения, которым он может управлять и количество данных, которые может хранить. Программное обеспечение и Данные хранятся в Модулях Памяти (MU). Компьютер может содержать количество MU, равное CPU x 40. Память может быть улучшена по цене 250 \$ за MU. CPU также определяет стартовый уровень Файрвола системы. Сила Файрвола равняется количеству CPU, работающих на нем. Компьютер с Мощностью выше 10 - Искусственный Интеллект с полной самостоятельностью и интерактивностью. Мощность может быть уменьшена с сокращением стоимости на 3000\$ за уровень.

Компьютер может также обладать умениями подобно персонажу. Память может быть использована как умение по курсу 1 MU на Уровень Навыка. Таким образом, компьютер может потратить 5 MU, чтобы иметь Навык Безопасности 5. Все компьютерные умения используют Мощность как первичную характеристику. Скорость используется, чтобы определить инициативу. Если используются Диаграммы Скорости, они могут использоваться, чтобы определить количество и порядок действий в ходе. Скорость может быть увеличена по цене 2000 \$ за единицу до +5.

Уровень Безопасности - навык Безопасности Сисадмина (компьютера), добавленный к его мощности при сопротивлении атакам. Уровень Безопасности используется также, чтобы определить Уровень Отслеживания сервера при использовании его в цепи соединений.

Компьютер может ответить хакеру автоматически. Как только Сканирующая программа обнаружила неправомерное вторжение, Компьютер может автоматически выполнять комплекс программ Антиперсонал против Хакера, или отследить сигнал и запустить программный комплекс Антисистема против компьютера Хакера.

Компьютер может также быть определен как Кибердека. Кибердеки или Кибермодемы - маленькие устройства, которые подобно компьютерам выполняют программы, но различны в том, что они связаны с пользователем путем вживления в мозг и использования неврологического управления. Кибердека, в современных терминах, немного больше чем жесткий диск и связь с сетью. Весь ввод и вывод обрабатываются мозгом пользователя.

Кибердеки не имеют CPU, но пользователь должен иметь Нейроинтерфейс и установленный процессор Кибермодема в мозгу, стоимость которого 1100\$ за аппаратную часть и 500\$ за хирургическую операцию. Кибердеки обеспечивают 10 MU, Скорость 0 и имеет силу Файрвола 2.

### **Прайс-лист на Компьютерное железо**

1 CPU 10,000\$ (Мощность 3, 40 MU, Сила Файрвол 1)

1 Кибердека 1000\$ (Мощность 0, 10 MU, Сила Файрвол 2)

+1 CPU 10,000\$ (Мощность +3 каждый, +40 MU каждый, Сила Файрвол +1 каждый, максимум 7 CPU)

+1 MU 250\$ (нет максимума)

+1 Скорость 2,000\$ (максимум +5)

-1 Мощность -\$3,000 (нет максимума, но не больше чем до -2. Вы может также покупать менее мощные CPU)

### **Кибердеки против Компьютеров**

В играх, где кибернетические интерфейсы обычны и более старые компы с ручным управлением редко встречаются, просто применяется модификатор -2 ко всем действиям, совершаемыми старыми компьютерами. В играх, где кибернетические интерфейсы редки (мир типа современного), применяется модификатор +2 ко всем действиям, совершаемым кибердеками.

Успешные нападения, сделанные против Кибердек с использованием комплекса программ Антисистемы, заставят мозг разорвать соединение и потерять сознание на 1d6 раундов.

### **Меню**

Чтобы упростить использование компьютера в контексте игры, обычно используется простой набор команд. Эти команды Называются "Меню". Хакер просто выбирает действие, основанное на списке, доступном из Меню.

#### **Меню:**

**Вход/Выход в систему:** Получение легального доступа к незащищенным данным Сервера через надлежащие методы авторизации (пароль, Установление подлинности LDL или биометрия).

**Запуск Программы:** Запустить внутреннее или внешнее приложение.

**Читать Файл:** Просмотреть содержимое файла данных, будь это Текст, Графика, Звук/Видео или Виртуальный мир.

**Копировать Файл:** Скопировать файл внешних данных на свой компьютер. Будьте осторожны, каждая операция копирования оставляет след в логе.

**Редактировать Файл:** Изменение содержания файла данных. Каждая модификация заносится в лог-файл, включая изменение самого лога.

**Удалить Файл:** Удалить файл данных. Все операции удаления сохраняются в лог, включая удаление самого лога.

**LDL:** Установить связь с Сервером. Будьте осторожны, если вы разорвали связь с сервером и Стелс бросок был провален, Сисадмин все еще может отследить ваш LDL.

### Программное обеспечение (Программы)

Приложения программного обеспечения характеризуются их Силой, которая действует как своего рода Точность Оружия и добавляется ко задачам, выполняемым этим приложением. Сила приложения оценивается от 1 до 10.

Программы также характеризуются Размером - количество Единиц Памяти, которое она использует на компьютере пользователя (имеет кумулятивный эффект). Так, компьютер с 30 Единицами Памяти MU) может содержать одну программу размером 15MU и три программы по 5MU одновременно. Отключение программы занимает одно действие.

Приложения могут иметь весьма специфичные эффекты, в зависимости от используемой программы. Наиболее обычные и широко-используемые приложения таковы:

Тип	Эффект	Сила	MU	Цена
Дешифратор (Decryption)	Вскрывает Гейты и Закрытые файлы.	4	2	400
Интродер (Intrusion)	Взлом файрвола.	4	1	400
Стелс (Stealth)	Обходит Программы Обнаружения.	3	1	300
Щит (Protection)	Защищает от програм Антиперсонала.	3	1	150
АнтиСистема (Anti-System)	Подвешивает/разрушает систему.	3	2	570
АнтиАйс (Anti-ICE)	Наносит 1дб, повреждений к STR отдельной программы	2	5	1320
АнтиПерсонал (Anti-Personnel)	Наносит 1д10 Хитов непосредственно пользователю, если связан через нейроразъем.	4	4	6750
Файрвол, Брэндмауер (Firewall)	Ограничивает доступ к защищенной информации.	POW +1	+1	+1000
Гейт, Авторизатор (Authentication)	Разрешает доступ к ограниченной информации избранным пользователям	2	1	2000
		+1	+1	+1000
Сканер (Detection)	Обнаруживает неправомерных пользователей, отслеживает сигнал и предупреждает Сисадмина.	4	5	720

Другое программное обеспечение, которое можно найти в системе Киберпанк 2020 полностью совместимо с этой системой.

### Утилиты

Утилиты - программы, которые помогают Хакеру в свободное от взлома время. Хотя они обычно не дают никакой практической пользы во время взлома, они тем не менее весьма полезны для обслуживания и подготовки компьютера хакера.

Тип	Эффект	Сила	MU	Цена
Восстановительные Утилиты (Restore Utility)	Перекомпилируют и восстанавливают разрушенные программы.	3	1	130
Регистрирующие Утилиты (Recorder Utility)	Ведут запись действий во время хака, для продолжения позже.	8	2	180
Антивирус	Обнаруживает и уничтожает Вирусные программы.	5	1	150
Утилиты Защиты Файлов (File Protection Utility)	Закрывает файлы данных подобно Гейту с силой 3	7	2	170
Архиваторы	Уменьшает размер программы в два раза. Требуется 2 хода для распаковки.	4	1	140

Резервирование данных (Backup Utility)	Создает копии большинства программ на чипе.	4	1	140
Картограф VR (VR Map Utility)	Определяет полную системную карту интерфейса VR.	6	3	200
Пакет Утилит	Все вышеуказанное в одном пакете. Экономит MU и Деньги.	5	10	1000

### Стандартное Программное обеспечение Хакера

Декриптор	(Сила 4, MU 2, 400 \$)
Интрудер	(Сила 4, MU 1, 400 \$)
Стелс	(Сила 3, MU 1, 300 \$)
Щит	(Сила 3, MU 1, 150 \$)
АнтиАйс	(Сила 2, MU 5, 1320 \$)
Итого	(MU 10, 2570 \$)

### Стандарт Программное обеспечение Защищенного Сервера

#### 1 - Обычные Системы

Сканер	(Сила 4, MU 5, 720 \$)
Итого	(MU5, 720 \$)

#### 2 - Серые Системы

Сканер	(Сила 4, MU 5, 720 \$)
Антисистема	(Сила 3, MU 2, 570 \$) Только Серые Системы
Итого	(MU 7, 1290 \$)

#### 3 - Черные Системы

Сканер	(Сила 4, MU 5, 720 \$)
Антисистема	(Сила 3, MU 2, 570 \$) Только Серые Системы
Антиперсонал	(Сила 4, MU 4, 6750 \$) Только Черные Системы
Итого	(MU 11, 8040 \$)

### Примеры Компьютеров:

#### 1 - Небольшая деловая или личная система (серая информация)

Статистика: POW 1 (1 CPU, -2 POW), MU 40, Скорость 0, 4000 \$

Пример: Незначительная Личная Информация, Палмтопы, Портативные Компьютеры.

#### 2 - Крупная деловая (серая информация) или личная система (черная информация)

Статистика: POW 3 (1 CPU), MU 40, Скорость 3, 16,000 \$

Пример: Деловые Счета, Секретная Личная Информация

#### 3 - Крупная деловая (черная информация) или Корпоративная система (серая информация)

Статистика: POW 6 (2 CPU), MU 80, Скорость 6, 32,000 \$

Пример: Альтернативные Счета, Информация Продаж для Клиентов

#### 4 - Правительственная (серая), Корпоративная (черная) или Криминальная система (серая информация)

Статистика: POW 9 (3 CPU), MU 120, Скорость 9, 48,000 \$

Пример: Полицейские Файлы, Холдинговая Информация

#### 5 - Правительственная (черная), Орбитальная (серая), или Криминальная система (черная информация)

Статистика: POW 10 (4 CPU, -2 POW), MU 160, Скорость 10, 54,000 \$

Пример: Файлы Секретных операций, Аккоунты пользователей, Лицевые Банковские Счета

#### 6 - Орбитальная система (черная информация)

Статистика: POW 12 (4 CPU), MU 160, Скорость 12, 64,000 \$

Пример: Орбитальные Базы данных, Искусственные Интеллекты.

## Товар

Как только Хакер успешно обошел системы безопасности (Файрвол, Гейт и Сканеры), он получает доступ к CPU защищенного сервера. Хакер может теперь просматривать содержимое файлов (текст, видео, звук, VR) или запускать онлайн-приложения.

Будьте осторожны, некоторые файлы могут иметь дополнительные меры безопасности. Например, файл с именем "Нелегальные Операции: Совершенно Секретно" может иметь отдельную программу-Сканер, прикрепленную к нему, которую Хакер должен предварительно обойти. Или файл может быть закрытым. Вмешательство в любую Айс программу автоматически требует обход Хакером Утилиты Защиты Файла и Сканера.

Обычные файлы данных, которые могут быть найдены на общем защищенном сервере:

- 1 Внутриофисные переговоры (Электронная почта)
- 2 Содействующие материалы (типа разработок VR симуляторов и Веб Страниц)
- 3 Деловые Отчеты (включая базы данных)
- 4 Финансовые Сделки
- 5 Серые Операции
- 6 Черные Операции

А также внутренние приложения для общего использования. Приложения могут быть от простых электронных таблиц и текстовых редакторов до VR симуляторов и управляемым компьютерным автоматизированным системам типа видеонаблюдения, управления лифтами, климатом, сборки роботов и т.д.

---

Обратите внимание на создании копий: В будущем Киберпанка, каждый файл имеет свой лог, неразрывно связанный с этим файлом, в котором записываются все действия с этим файлом. И хотя сам лог тоже может быть модифицирован, в логе останется запись об этой модификации.

Эта особенность используется, чтобы определить ценность данных. Например, хакер находит файл, названный "Баня. Совершенно Секретно." в некоей базе данных. Лог для этого файла укажет, сколько раз, он просматривался, кем и когда. Наш Хакер решает сделать копию. Оригинал теперь делает запись в лог, что с него была снята копия тогда-то и тем-то. Копия делает запись в свой лог, что она была скопирована с оригинала тогда-то тем-то. Каждый раз, когда хакер открывает файл для просмотра, лог записывает, что файл просматривался в такое-то время таким-то пользователем.

Если Хакер желает продать эту информацию, предполагаемый покупатель может просмотреть лог файла и увидеть, сколько раз файл был просмотрен, изменен и скопирован и кем. Разбавленные данные понизят ценность файла. Девственно чистые данные повысят его ценность. Предприимчивый Хакер может легко изменить лог файла, однако будет сделана запись, что лог был изменен, что приведет к еще большему падению стоимости.

Хакер может попробовать удалить запись о изменении, однако эта операция также отразится в логе. Это неразрывный круг. Самое лучшее в этой ситуации – сделать одну копию и не просматривать ее.

---

## **Порядок Взлома Защищенного Сервера:**

**1.** Библиотечные Исследования (Интеллект + Библ.Исследования + 3d6 против Уровень сложности) чтобы собрать немного фактов о Корпорации. Число переброса при успехе предоставляется, как премия к Декриптору в третьем шаге.

**1a.** Хакер загружает выбранный софт. Необходимый минимум включает один Декриптор, один Интродер, один Стелс, один АнтиАЙС и один Щит.

**2.** LDL (Бросок 1d10 против Уровня Безопасности LDL). Хакер соединился с отдаленным сервером и может использовать его LDL для соединения с другим отдаленным сервером, создавая цепь соединений к цели. Сисадмины должны проследить каждое соединение, чтобы определить LDL Хакера. Как только цепь соединений установлена, Хакер может использовать эту цепь неопределенно долго, если доступ не прерывается провайдером отдаленного Сервера Сети.

Если бросок провален, отдаленный сервер отказал в подключении Хакеру. В этом случае, Хакер должен сделать последнее подключение к Серверу назначения.

**3.** Декриптор против Гейта (Интеллект + Хакерство + Сила Декриптора + 3d6 против Мощность + Безопасность + Сила Гейта + 3d6).

Если бросок успешен, Хакер обманул Гейт и получает разрешение на доступ к Серверу. Хакер все еще может быть отслежен Сканерами.

Перейти на шаг 4.

Если неудачно, Хакер все еще не имеет доступа к Серверу. Повторение неудавшейся попытки (3d6) вызовет срабатывание Сканера, приведя в готовность Сисадмина, который может использовать Сканеры для отслеживания расположения и/или мониторинг действий Хакера. Перейти на шаг 4.

**4.** Интродер против Файрвола (Интеллект + Хакерство + Сила Интродера + 3d6 против Мощность + Безопасность + Сила Файрвола + 3d6).

Если бросок успешен, Файрвол обойден и хакер теперь имеет доступ к серверу. Однако, Хакер все еще может быть отслежен Сканерами. Перейти на шаг 5.

При неудаче, Хакер все еще не имеет доступа к серверу, но, возможно, был замечен.

Если незамечен, можно попытаться снова.

Если замечен, то либо Сисадмин, либо Программа Антиперс уведомляется о присутствии Хакера, и попытается проследить или воспрепятствовать ему. Перейти к разделу Бой.

**5.** Стелс против Сканера (Интеллект + Хакерство + Сила Стелс + 3d6 против Мощность + Безопасность + Сила Сканера + 3d6).

Если бросок успешен, Сканер не обнаружил никакой неправомерной деятельности, но может провести повторную проверку пользователя по истечении некоторого времени (3d6 раундов). Перейти на шаг 6.

При неудаче, Сканер обнаружил неправомерную деятельность и может уведомить Сисадмина или Программу Антиперс. Перейти к разделу Бой.

**6.** Теперь вы имеете доступ к серверу. Компьютер думает, что Вы зарегистрированы как официальный авторизованный пользователь. Вы можете использовать файлы данных и софт, доступные на этом сервере. Некоторые файлы данных и приложения могут содержать дальнейшие меры безопасности. Если так, повторите шаг 3.

**7.** Заметание следов. Неудачный выход или разрыв линии означает, что Сисадмин все еще может проследить ваше местоположение. Старайтесь всегда выходить должным образом. Вы можете просмотреть содержание любого файла, который вы загрузили, но опасайтесь логов: Не обесценьте ваши данные!

## **Бой!**

### **1. Инициатива.**

Человеческий Интеллект + Скорость Компьютера + 3d6

Мощность Компьютера + Скорость + 3d6

**2.** Проигравший первый делает заявку, Победитель первый действует. Поэтому, если проигравший запускает Программу Антиперс на вторгшегося, победитель может либо активизировать подходящую защиту, либо рискнуть и напасть на проигравшего первым.

### **3. Боевые опции:**

**3a.** Вторгшийся нападает на Айс. (Интеллект + Хакерство + Сила Антиайса + 3d6 против Мощности Компьютера + Безопасность + Сила Программы + 3d6).

При успехе, софт разрушен и стерт с сервера.

При неудаче, нападение отражено, нападающая программа разрушена. Сканер автоматически отслеживает соединение Хакера и сигнализирует Сисадмину, который может попытаться воспрепятствовать Хакеру.

**3b.** Вторгшийся нападает на Сисадмина, или Сисадмин нападает на Вторгшегося. (Интеллект + Хакерство/Безопасность + Сила Анти-Перса + 3d6 против Сила Программы Защиты + Интеллект + Хакерство/Безопасность + 3d6)

При успехе, Программа Антиперсонала наносит ущерб непосредственно мозгу пользователя (Сила Антиперса - Сила Щита в Хитах), только если соединен через нейроразъем. На более старых компьютерах без нейроуправления, обращайтесь с нападением как с атакой Антисистемы.

При неудаче нападение не сумело нанести какой-либо ущерб.

**3c.** Защита CPU нападает на Вторгшегося. (Мощность + Безопасность + Сила Программы Антиперсонала + 3d6 против Интеллект + Хакерство + Сила Защитной Программы + 3d6)

При успехе, программа Антиперсонала наносит ущерб непосредственно мозгу пользователя (Сила Антиперса - Сила Щита в Хитах), только если соединен через нейроразъем. На более старых компьютерах без нейроуправления, обращайтесь с нападением как с атакой Антисистемы.

При неудаче нападение не сумело нанести какой-либо ущерб.

**3d.** Вторгшийся нападает на Систему. (Интеллект + Хакерство + Сила Программы + 3d6 против Мощности Компьютера + Безопасность + Сила Файрвола + 3d6)

При успехе, Антисистемный софт разрушает CPU, прекращая всю деятельность до того момента, пока CPU не сможет быть перезапущена с использованием Утилит Восстановления. Вторгшийся немедленно разъединяется, но не выходит. Как только CPU перезапускается, Сисадмин может сделать попытку отследить соединение. Если цель использует Больше чем 1 CPU, все CPU должны быть нейтрализованы, чтобы разрушить систему.

При неудаче, нападение против CPU потерпело неудачу. Сканер автоматически приводит в готовность Сисадмина

**3e.** Сканер отслеживает Вторгшегося (Мощность + Безопасность + Сила Программы + 3d6 против Интеллект + Хакерство + Уровень отслеживания + 3d6)

При успехе Сканер распознал происхождение соединения Хакера и информирует Сисадмина. Сканер должен проследить каждое соединение в цепочке (См. выше) чтобы отследить истинное происхождение. После определения, Сисадмин может уведомить провайдера Хакера о его незаконных действиях. Кроме того, любые дальнейшие попытки соединиться через любой сервер отслеженной цепочки автоматически активирует Сканерный софт Сисадмина, сообщив о попытке неправомерного доступа. Если связь была разъединена без надлежащей процедуры выхода, Сисадмин все еще может отследить это соединение.

При неудаче, Сканер не преуспевает. Однако может пытаться отследить соединение каждый раунд.

**3.** Ущерб. Ущерб причиняется воздействуемым системам или программам (или Хиты в случае Черного Айса).

## Словарь

Анти-Айс софт, Ледокол (Anti-ICE Software): Софт для разрушения или удаления другого софта.

Анти-Персонал софт (Anti-Personnel Software): Софт для причинения ущерба пользователю нейроинтерфейса.

Анти-Систем софт (Anti-System Software): Софт для разрушения или остановки CPU другого компьютера.

Искусственный интеллект (Artificial Intelligence, AI): Продвинутый компьютер, способный к полному взаимодействию и принятию решений.

Черная Информация/Система (Black Info/System): Высшая Секретная информация. Секретность вплоть до убийства для предотвращения разглашения. Защищенные сервера со смертоносным софтом типа Антиперсонал.

Гейт (Codegate): Киберпанковское название опознавательного механизма. Гейт может проверять комбинации типа логин/пароль, адрес соединения (LDL), отпечатки пальцев, сетчатка глаза, голосовые проверки, DNA, и т.д.

ЦПУ (CPU): Центральное Процессорное Устройство, мозг компьютера. Многие компьютеры имеют дополнительные CPU, что увеличивает их Мощность. Кроме того, если ЦПУ выходит из строя, компьютер может продолжать работать на уменьшенном уровне.

Кибердека (Cyberdeck): или Кибермодем, компьютерное устройство, которое использует мозг оператора как CPU.

Файл данных (Datafile): Любой файл, который содержит информацию. Файлы данных могут содержать текст, графику, видео, звук или полносенсорный ВР (VR)

Защищенный сервер, Инфофорт (datafortress): Сервер, который предоставляет доступ к информации только уполномоченным пользователям.

Сервер Данных (Datasever): Компьютер, обеспечивающий доступ к данным по запросу. Брэндаер, Файрвол (Datawall): Термин Киберпанка для Firewall. Файрвол без Гейта просто запрещает доступ к информации и должен быть пройден с помощью софта типа Интродер.

Дешифратор (Decryption Software): Программное обеспечение, разработанное для обмана Гейтов.

Сканер, Детектор (Detection Software): Программное обеспечение, которое периодически перепроверяет пользователей на сервере, для подтверждения их прав доступа. Если обнаружен неправомерный доступ, Сканер уведомляет Сисадмина или автоматически разворачивает софт типа Анти-Персонал или Анти-система в зависимости от конфигурации сервера.

Серая Информация/Система (Grey Info/System): Секретная информация. Не настолько секретная, чтобы доводить дело до убийства. Сервера с несмертельными контрмерами против вмешательства (софтом типа Антисистема).

Хакер (Hacker): Человек, вламывающийся в закрытые сети для получения информации или удовольствия от своих действий.

Хакерство (Hacking): Навык, используемый Хакерами. В терминах игры, Хакерство и Безопасность - тот же самый навык, используемый для разных целей.

Айс (ICE): Intrusion Countenance Electronics. Система противодействия вторжению. Сокращение для программы защиты сети. Предназначена для предотвращения любого нелегального доступа к данным сервера.

Иконка (Icon): Визуальное представление. В Киберпанке относится к 3D представлению компьютерного объекта. Файл может быть представлен иконкой, щелкнув/захватив/потянув/открыв которую можно увидеть содержание этого файла. Часто, события также предоставляются иконками. Например, Сисадмин может представить свое присутствие на сервере иконкой рыцаря в броне. Если Хакер видит рыцаря в броне, то он знает, что Сисадмин вошел на сервер.

Корпорация Интернет (Internet Corporation): Творение Киберпанка – конгломерат Сетевых Провайдеров. В современном мире, это может быть несколько компаний типа MCI, UUNet, и т.д.

Интродер софт (Intrusion Software): Программы для временного обезвреживания Файрвола, тем самым обеспечивая доступ к серверу. Их недостаток в том, что их использование может активировать Сканер.

LDL: Эквивалент современного IP адреса. В Киберпанке, LDL служит также как универсальный телефонный номер, адрес электронной и голосовой почты.

Единица Памяти (Memory Unit, MU): В Киберпанке эквивалент Мегабайта. Не имеет никакого реального соответствия и используется как некая абстрактная единица памяти.

Обычная Информация/Система (Mundane Info/System): Конфиденциальная информация, но едва ли секретная. Ограниченная информация, которая однако не охраняется особыми контрмерами. Сервера, которые используют только Сканеры.

Сеть (Net): Эквивалент Интернета. В Киберпанке Сеть представлена 3D полносенсорным виртуальным миром. Другие названия Сети: Киберпространство, Интерфейс, Веб, Паутина и т.д.

Провайдер Доступа в Сеть (Net Access Provider): Компания, у которой пользователи арендуют временный LDL. Корпорация Интернет - крупный Провайдер. Провайдеры в основном сотрудничают с Сисадминами для воспрепятствования деятельности Хакеров. Если Провайдер получает информацию, что один из его пользователей, возможно, Хакер, он прекращает обслуживание этого пользователя. Эквивалент современных провайдеров Интернета.

Пользователь Сети (Netuser): Любой, легально использующий Сеть. Эквивалент современным серверам Сети.

Мощность (Power): В механике Fuzion - относительная мера способностей компьютера.

Уровень Безопасности (Security Level): В механике Fuzion представляет навык, используемый Сисадмином или Компьютерным CPU, чтобы обнаружить или захватить Хакера. В терминах игры, Безопасность и Хакерство - один и тот же навык, используемый для различных целей.

Сервер (Server): Компьютер, связанный с Сетью. Сервер действует как посредник между запросом человека о какой-либо информации и памятью, хранящей информацию. Ваш компьютер посылает запрос серверу, тот находит ее и посылает на ваш компьютер.

Скорость (Speed): В механике Fuzion - относительная мера скорости компьютера.

Стелс Софт (Stealth Software): Программное обеспечение, которое пытается обмануть Сканер путем подтверждения авторизации или игнорирования Хакера.

Сила (Strenght): В игровой механике Fuzion - относительная мера способностей программы.

СисАдмин (SysAdmin): Администратор Системы. Человек, отвечающий за поддержание безопасности защищенного сервера.

Система (System): Собрание компьютерных компонентов и их общая работа. Группа компьютеров, соединенных в единую сеть - система. Сеть в целом может рассматриваться очень большой системой.

Уровень Отслеживания (Trace Value): Относительная трудность в отслеживании происхождения соединения.

Интерфейс Виртуального Мира, Виртуальный Интерфейс (Virtual Reality Interface): Во многом подобен современному Графическому Пользовательскому Интерфейсу (GUI), Виртуальный Интерфейс показывает "Рабочий стол" компьютера как трехмерную интерактивную вселенную вокруг пользователя. В Киберпанке, к Сети можно обращаться с помощью подобного интерфейса, где Сетевые LDL показаны как Иконки вокруг пользователя. Пользователь свободно перемещается в этом месте, выбирая желаемые действия, входя в контакт с иконками руками.

ВМ Конструкции (VR Construct): 3D Изображение в Виртуальном Интерфейсе. Конструкции могут быть чем угодно, ограниченные только воображением их создателя. Их размер определяется тем, сколько памяти они требуют. ВМ Симулятор (VR Sim): VR Моделирование. Крошечная виртуальная вселенная. В Киберпанке, ВМ Симулятор может быть интерактивной игрой, рекламным объявлением, областью конференции сети или детской площадкой. Любая ситуация, в которой вам нужно попасть куда-нибудь, где физически вы не можете пребывать, может быть решена с помощью ВМ Сима.