**“Белые хакеры”**

[1. Каким образом и насколько в странах легализованы «белые хакеры»? (обязательная ли это процедура или по желанию, если по желанию, то зачем это хакерам) 2](#_u5qy71aw3dnh)

[2. Существуют ли официальные реестры хакеров? 5](#_kgxzo08f6wvm)

[3. Есть ли сертификация белых хакеров? Какая чаще используется: принудительная или необязательная? 5](#_oh55sl5c2eh9)

[4. Какая ответственность (уголовная, административная и тд) есть за «черное хакерство» и каким образом разделяется белое и черное (что можно, что нельзя)? 6](#_6nzlevomklta)

[США 6](#_smn286fqq5oh)

[UK 13](#_aydbhg9pw0o7)

[ГЕРМАНИЯ 14](#_j7dpdirqrudk)

[ОАЭ 14](#_amp66wkmd5rs)

[ИЗРАИЛЬ 15](#_96iuyysx5pwf)

[ПАКИСТАН 16](#_4qfwjykhk5zn)

[5. Как регламентируются пентесты и баг-баунти государственных структур КИИ - какие требования к верификации хакеров? 17](#_vate8xpgpg57)

[6. Как законодательно регулируется деятельность баг-баунти платформ? Верифицируют ли платформы хакеров и нужно ли хакером давать о себе полную информацию до выплаты (в момент поиска уязвимости) или везде они действуют анонимно до момента выплаты, как сейчас в РФ? 18](#_j2a02o76jc3s)

Несмотря на все меры предосторожности, системы и IT продукты редко бывают полностью свободны от уязвимостей безопасности. Для того чтобы обнаружить и устранить уязвимости и области атак на ранней стадии, программное обеспечение и оборудование должны выдерживать тестирование безопасности. Однако, исследователи кибербезопасности, которые сообщают об уязвимостях в интересах общего блага (так называемые «белые хакеры»), в настоящее время во многих странах действуют, неся риск уголовного преследования.

В одних странах пентесты (тестирование на проникновение) широко распространены и поощряются, в других - запрещены. Несанкционированное тестирование в таких странах может повлечь за собой серьезные правовые последствия, включая крупные штрафы, тюремное заключение и депортацию иностранных граждан. Поэтому частные лица и организации должны понимать правовые и нормативные рамки различных стран, регулирующие тестирование на проникновение (пентест).

Тест на проникновение или пентест — это смоделированная кибератака на компьютерную систему заказчика для проверки уязвимостей. Тестирование на проникновение, может включать в себя различные методы тестирования, включая внешнее тестирование, внутреннее тестирование, слепое тестирование, двойное слепое тестирование и целевое тестирование. Эти процедуры тестирования обычно подразумевают выявление и эксплуатацию уязвимостей системы контролируемым и безопасным образом.

# **Каким образом и насколько в странах легализованы «белые хакеры»? (обязательная ли это процедура или по желанию, если по желанию, то зачем это хакерам)**

Безопасное программное обеспечение появляется после постоянного выявления и исправления

ошибок. Эта проверенная временем стратегия в арсенале методов разработки безопасности программного обеспечения привлекла внимание СМИ в начале 2000-х годов, когда самоназванные «белые хакеры» взломали программное обеспечение, а затем обратились к производителю программного обеспечения с предложением раскрыть ошибку в обмен на оплату или даже работу. Однако прошли те дни, когда такие белые хакеры могли рассчитывать на то, что их наймут после взлома приложения.

Типы хакеров:



Страны, где пентесты строго регулируются:



1. **Великобритания** — В 1990 году был создан Закон о неправомерном использовании компьютеров (CMA) для регулирования законного доступа к компьютерным данным. Этот закон запрещает несанкционированный доступ к данным и изменение хранимой информации без согласия владельца. Согласно CMA, получение несанкционированного доступа к компьютерным системам является незаконным. Национальный центр кибербезопасности Великобритании (NCSC) также руководит тем, как организации могут проводить тестирование на проникновение законно и этично.
2. **Индия** — Перед проведением теста на проникновение в Индии тестировщик должен получить разрешение от руководства. Затем тест должен проводиться в рамках предопределенных ограничений. Различные правовые и нормативные рамки регулируют деятельность по тестированию на проникновение в Индии, включая Закон об ИТ, IPC, руководящие принципы RBI, Национальную политику кибербезопасности и PCI DSS.
3. **Сингапур** — Согласно разделу 3(1) Закона о неправомерном использовании компьютеров 1993 года («CMA»), незаконно, чтобы кто-либо намеренно заставлял компьютер выполнять любую задачу для получения несанкционированного доступа к программе или данным, хранящимся на компьютере. Тестирование на проникновение допускается только с явного разрешения владельца тестируемой системы. Оно должно соответствовать рекомендациям Агентства кибербезопасности Сингапура (CSA).
4. **США** — Закон о компьютерном мошенничестве и злоупотреблении 1986 года (CFAA) запрещает доступ к компьютерным системам без разрешения, что включает в себя тестирование на проникновение. Закон о конфиденциальности электронных коммуникаций (ECPA) также запрещает тестирование на проникновение. NIST публикует различные стандарты и руководства по кибербезопасности, в том числе связанные с тестированием на проникновение.
5. **Япония** — В Японии несколько законов и нормативных актов регулируют деятельность по тестированию на проникновение. Основными законами, регулирующими тестирование на проникновение в Японии, являются Закон о защите личной информации (APPI) и Закон о сетях информации и связи (ICNA).
6. **Канада** — Проведение несанкционированного тестирования на проникновение может считаться нарушением в соответствии с Уголовным кодексом Канады.
7. **Австралия** — Проведение тестирования на проникновение в систему или сеть без получения согласия ее владельца или администратора классифицируется как несанкционированный доступ, нарушение федерального Закона об уголовном кодексе 1995 года, и, следовательно, считается незаконным.
8. **Франция** - Во Франции при проведении тестирования на проникновение необходимо соблюдать требования законодательства, включая Закон о защите данных Франции, Уголовный кодекс Франции, Общий регламент по защите данных (GDPR) и руководящие принципы, установленные ANSSI. Кроме того, тестирование должно быть разрешено владельцем системы и проводиться с согласия лиц, работающих в системе.
9. **Южная Корея** — Основным законом, регулирующим тестирование на проникновение в Южной Корее, является Закон о содействии использованию информационно-коммуникационных сетей и защите информации (далее именуемый «Закон о сетях») и Указ о применении Закона о сетях.
10. **Китай** — Положения о надзоре и инспекции безопасности в Интернете органами общественной безопасности. Эти положения дают полиции и другим органам общественной безопасности полномочия проводить инспекции и расследования в области кибербезопасности, включая пентесты, в отношении компаний, работающих в Китае. Другие организации должны получить необходимые разрешения и одобрения от соответствующих органов перед проведением любых мероприятий по пентестам, чтобы избежать нарушения этих законов и правил.

Кроме того, Китай передал на аутсорсинг компоненты киберопераций своих военных разведывательных сообществ, продвигая «патриотический хакеризм» для поддержки усилий страны по подготовке к потенциальному конфликту или во время него.

1. **Россия:** Главным нормативным актом страны, регулирующим информационную безопасность, является Федеральный закон «О технической защите информации» №149-ФЗ, который определяет стандарты защиты информации. Согласно этому закону, любое испытание на проникновение требует одобрения владельца проверяемой системы. Кроме того, только лицензированные охранные фирмы или лица, обладающие необходимыми техническими знаниями и опытом, имеют право проводить такие испытания.

**Страны, где пентесты являются законными (есть отсылка в кодексе на пентесты).**

1. **Германия:** В Германии тестирование на проникновение регулируется немецким уголовным кодексом (StGB) и немецким федеральным законом о защите данных (BDSG). Перед проведением любого тестирования на проникновение необходимо получить разрешение от владельца ИТ-инфраструктуры.
2. **Нидерланды:** Уголовный кодекс Нидерландов допускает этичный хакерский взлом с согласия владельца.
3. **Швейцария:** Уголовный кодекс Швейцарии разрешает этичный взлом, если лицо, осуществляющее взлом, имеет законные полномочия или согласие владельца.

Правительство Мальты работает над созданием правовой базы, которая будет поддерживать этичную практику хакерства. Предлагаемые изменения появились после того, как два года назад [против трех студентов факультета компьютерных наук Мальтийского университета и их преподавателя были выдвинуты уголовные обвинения.](https://lovinmalta.com/malta/ksu-calls-for-legal-reform-to-protect-ethical-hacking-as-charged-lecturer-and-former-students-receive-support/) Они обнаружили недостатки в FreeHour, крупнейшем студенческом приложении Мальты.

# **2. Существуют ли официальные реестры хакеров?**

Ни в одной из проанализированных стран, такого реестра не было найдено.

# **3. Есть ли сертификация белых хакеров? Какая чаще используется: принудительная или необязательная?**

Сертификации для белых хакеров играют важную роль в подтверждении их навыков и знаний в области кибербезопасности. Кроме того. Эти сертификации часто включают в себя инструкции по правовым и этическим соображениям, относящимся к профессии.

Среди наиболее широко признанных сертификаций в этой области — Certified Ethical Hacker (CEH) от Совета ЕС, Offensive Security Certified Professional (OSCP), Certified Penetration Tester (CPT).

**Сертификация CEH (Certified Ethical Hacker)**, является одной из самых известных и признанных сертификаций в области этичного хакинга. Она предоставляется организацией EC-Council и охватывает широкий спектр тем, связанных с кибербезопасностью. CEH предназначена для специалистов, которые хотят углубить свои знания в области защиты информации и научиться выявлять уязвимости в системах.

**Сертификация OSCP (Offensive Security Certified Professional)** предоставляется организацией Offensive Security и ориентирована на практическое применение навыков в области этичного хакинга. Она считается одной из самых сложных и престижных сертификаций в этой области. OSCP требует от кандидатов глубоких знаний и умений, а также способности применять их в реальных условиях.

**Certified Penetration Tester (CPT)**  предназначена для сотрудников службы безопасности, чьи должностные обязанности включают оценку целевых сетей и систем для поиска уязвимостей безопасности.

Другие популярные сертификации:

**CISSP (Certified Information Systems Security Professional)**

Сертификация CISSP предоставляется организацией (ISC) и охватывает широкий спектр тем в области информационной безопасности. Она предназначена для опытных специалистов и требует не менее пяти лет опыта работы в сфере безопасности. CISSP охватывает такие темы, как управление рисками, разработка и управление программами безопасности, а также правовые и нормативные аспекты информационной безопасности.

**GPEN (GIAC Penetration Tester)**

Сертификация GPEN предоставляется организацией GIAC и ориентирована на специалистов по тестированию на проникновение. Она охватывает такие темы, как методы взлома, эксплуатация уязвимостей и отчетность. GPEN предназначена для специалистов, которые хотят углубить свои знания в области тестирования на проникновение и научиться выявлять уязвимости в системах.

**В РФ**

Легализация деятельности белых хакеров, проверяющих надежность ИБ-защиты корпоративных и государственных IT-систем, обсуждается с лета 2022 года. Тогда Минцифры начало прорабатывать возможность введения понятия bug bounty в правовое поле. Предполагалось внести изменения в закон «Об информации, информационных технологиях и о защите информации» и статью 272 УК РФ «Неправомерный доступ к компьютерной информации».

В декабре 2023 года в Госдуму была внесена версия законопроекта. Проект вносил изменения в Гражданский кодекс РФ, вводя понятия [«белый хакер»](https://www.securitylab.ru/glossary/belyy_khaker/) и bug bounty, а также определял сроки уведомления компании в случае обнаружения уязвимости. По мнению законотворцев, предложенные меры по созданию реестра и сертификации должны обезопасить работу bug bounty со значимыми объектами, включая критическую информационную инфраструктуру (КИИ), позволит легализовать многие направления, связанные с наступательной и превентивной безопасностью, а также устранить серые зоны, в которых сейчас находятся белые хакеры.

Слабые места инициативы.

* В текущей геополитической ситуации публично доступный реестр белых хакеров может стать важным источником информации для противоположной стороны.
* Кроме того, жесткие бюрократические требования к процедуре вступления в ряды белых хакеров для участия в программах bug bounty могут отпугнуть потенциальных участников. Также есть риск, что в таком случае найденные уязвимости хакеры будут продавать не компаниям за вознаграждение, а злоумышленникам.
* Мало хакеров захочет серьезно заниматься анализом защищенности КИИ и других систем, если для этого потребуется находиться в реестре.
* Также реестры часто становятся объектом утечек, что может представлять серьезную опасность для людей, находящихся в них. Существуют опасения, что против таких специалистов могут быть введены персональные санкции США и других стран, а их жизни могут подвергаться опасности.

# **4. Какая ответственность (уголовная, административная и тд) есть за «черное хакерство» и каким образом разделяется белое и черное (что можно, что нельзя)?**

# 

## **США**

Киберпреступления регулируются как федеральными законами, так и законами штатов. Закон о компьютерном мошенничестве и злоупотреблениях (The Computer Fraud and Abuse Act, CFAA 1984) устанавливает, что киберпреступления являются федеральными преступлениями. В этом законе детализируются идентификация федеральных киберпреступлений и меры наказания за их совершение. Также, США подписали Конвенцию о киберпреступности в 2006 году, и США внедрили положения в федеральный закон.

**Закон о компьютерном мошенничестве и злоупотреблениях — Computer Fraud and Abuse Act (CFAA)**

Закон США о компьютерном мошенничестве и злоупотреблениях (The United States Computer Fraud and Abuse Act, 18 U.S.C. § 1030, также известный как Title 18 U.S.C. Section 1030), является федеральным антихакерским законом. Поправка, внесенная в 1986 году к Закону о контрафактных устройствах доступа и злоупотреблениях (Counterfeit Access Device and Abuse Act), принятому в 1984 году, делает незаконным намеренный несанкционированный доступ к компьютеру. Позже в закон было включено такое преступления, как кража личных данных.

**Национальный закон об информационной инфраструктуре — National Information Infrastructure Act (NIIA)**

В 1996 году был принят Закон о национальной информационной инфраструктуре, который расширил сферу действия CFAA, включив в него несанкционированный доступ к защищенному компьютеру без соответствующих прав, предусмотренных сторонами. До этого изменения подобные действия считались преступлением по CFAA только, если они были совершены для коммерческой выгоды. В соответствии с NIIA несанкционированный доступ без соответствующего разрешения противоречит закону, даже если это всего лишь просмотр информации, находящейся на компьютере, без какой-либо финансовой выгоды.

**Виды федеральных киберпреступлений**

**Согласно CFAA, существует семь видов деятельности, связанных с компьютерами, которые определены как преступные:**

| 1030(a)(1) | несанкционированный доступ к компьютеру для получения информации о национальной безопасности с намерением причинить вред Соединенным Штатам или в интересах иностранного государства |
| --- | --- |
| 1030(a)(2) | несанкционированный доступ к компьютеру для получения защищенной финансовой или кредитной информации |
| 1030(a)(3) | несанкционированный доступ к компьютеру, используемому федеральным правительством |
| 1030(a)(4) | несанкционированный доступ к защищенному компьютеру с целью обмана |
| 1030(a)(5) | преднамеренное повреждение защищенного компьютера |
| 1030(a)(6) | использование в мошеннических целях компьютерных паролей и любой другой информации, которая может быть использована для получения доступа к защищенному компьютеру |
| 1030(a)(7) | угроза защищенному компьютеру с целью вымогательства денег или каких-либо иных ценностей |

“Защищенный компьютер” в соответствии с 1030(a)(7) – это компьютер, используемый правительством США, финансовым учреждением или используемый в иностранной или межгосударственной торговле, или связи.

**Наказания за совершение киберпреступления на федеральном уровне**

Руководство по вынесению приговоров в США (The United States Sentencing Guidelines) содержит руководящие указания по установлению мер наказания за совершение федеральных киберпреступлений. Руководящие принципы не являются обязательными, скорее они действуют в качестве рекомендации для вынесения приговора. Это сложная система, которая использует Базовый уровень правонарушения (Base Offense Level) в соответствии с федеральным законом и последующее увеличение наказания в зависимости от финансовых потерь потерпевшего или потерпевших. В зависимости от суммы ущерба и совершенного преступления осужденному за совершение киберпреступления может грозить более 20 лет лишения свободы.

**Виды киберпреступлений согласно законодательству Нью-Йорка**

| **Пенитенциарный код штата Нью-Йорк** | **Тип** | **Классификация** | **Описание** |
| --- | --- | --- | --- |
| PL 156.05 | Несанкционированное использование компьютера | преступление небольшой тяжести – Class A Misdemeanor | Физ лицо сознательно несанкционированно использует, или осуществляет доступ к компьютеру, компьютерному сервису или компьютерной сети. |
| PL 156.10 | Взлом чужого компьютера | Тяжкое преступление – Class E Felony | Физ лицо сознательно несанкционированно использует, провоцирует использование или осуществляет доступ к компьютеру, компьютерной службе или компьютерной сети и:  1. Делает это с намерением совершить или попытаться совершить или содействовать совершению какого-либо тяжкого преступления; или же  2. Сознательно осуществляет доступ к компьютерным материалам. |
| PL 156.20 | Вмешательство в компьютер четвертой степени | преступление небольшой тяжести – Class A Misdemeanor | Физ лицо провоцирует несанкционированное использование или осуществляет несанкционированный доступ к компьютеру, компьютерной службе или компьютерной сети и преднамеренно изменяет или уничтожает компьютерные данные или компьютерную программу другого лица. |
| PL 156.25 | Вмешательство в компьютер третьей степени | Тяжкое преступление – Class E Felony | Физ лицо осуществляет преступное вмешательство в компьютер четвертой степени и:  1. Имеет намерение совершить, предпринимает попытку совершить или совершает тяжкое преступление; или  2. Ранее был осужден за компьютерное преступление; или  3. Преднамеренно изменяет или разрушает компьютерный материал; или  4. Преднамеренно изменяет или уничтожает компьютерные данные или компьютерную программу, причинив ущерб, превышающий $1,000. |
| PL 156.26 | Вмешательство в компьютер второй степени | Тяжкое преступление – Class D Felony | Физ лицо осуществляет преступное вмешательство в компьютер и преднамеренно разрушает или изменяет:  1. Компьютерные данные или компьютерную программу, причинив ущерб, превышающий $3,000; или  2. Компьютерный материал, содержащий медицинские записи (история болезни, лечение и т. д.) идентифицируемого лица, что привело к серьезной физической травме этого лица, о риске получения которой обвиняемому было известно и он сознательно не принимал его во внимание. |
| PL 156.27 | Вмешательство в компьютер первой степени | Тяжкое преступление – Class C Felony | Человек совершает преступное вмешательство в компьютер и преднамеренно изменяет или уничтожает компьютерные данные или компьютерную программу, причинив ущерб, превышающий $50,000. |

В [**Article 156 of New York Penal Law**](http://ypdcrime.com/penal.law/article156.htm#p156.00) перечислены несколько различных типов киберпреступлений, от малой тяжести до очень серьезного тяжкого преступления. Некоторые из мер наказания предусматривают денежную компенсацию.

Другими типами кибер-преступлений, в соответствии с законодательством штата Нью-Йорк, являются: незаконная загрузка материалов, защищенных авторским правом (пиратство); использование вредоносного программного обеспечения; кибер-преследование; детская порнография; кража личных данных.

Меры наказания за совершение Киберпреступления в Штате Нью-Йорк

Согласно New York State Penal Law Articles 70 и 80 осуждение за киберпреступление может повлечь за собой штраф, тюремное заключение или и то, и другое. При принятии решения судья учитывает много факторов. Наличие у обвиняемого предыдущих судимостей за киберпреступления или любые другие преступления может оказать существенное влияние, особенно если эти судимости включали в себя жестокие тяжкие преступления, повторяющиеся преступления или повторяющиеся жестокие тяжкие преступления. Кроме того, судья примет во внимание личность жертвы и тяжесть последствий совершенного преступления. Решение о том, получит ли обвиняемый максимальное наказание за компьютерное преступление, остается на усмотрение судьи

| **Классификация** | **Максимальный штраф** | **Максимальный срок** |
| --- | --- | --- |
| Тяжкое преступление – Class B Felony | $5,000 или удвоенная сумма выгоды, полученной обвиняемым в результате совершенного преступления | 25 лет |
| Тяжкое преступление – Class C Felony | $5,000 или удвоенная сумма выгоды, полученной обвиняемым в результате совершенного преступления | 15 лет |
| Тяжкое преступление – Class D Felony | $5,000 или удвоенная сумма выгоды, полученной обвиняемым в результате совершенного преступления | 7 лет |
| Тяжкое преступление – Class E Felony | $5,000 или удвоенная сумма выгоды, полученной обвиняемым в результате совершенного преступления | 4 года |
| преступление небольшой тяжести – Class A Misdemeanor | $1,000 | 1 год |
| преступление небольшой тяжести – Class B Misdemeanor | $500.00 | 3 месяца |

## **UK**

В UK хакерство, как правило, считается незаконным. [Закон о неправомерном использовании компьютеров 1990 года](https://nationalcrimeagency.gov.uk/who-we-are/publications/523-cyber-choices-hacking-it-legal-computer-misuse-act-1990/file#:~:text=The%20Computer%20Misuse%20Act%201990%20was%20created%20to%20deal%20with,or%20modifying%20data%20without%20permission.&text=Unauthorised%20access%20to%20computer%20material.&text=You%20watch%20your%20friend%20enter,and%20read%20all%20their%20messages.) (The Computer Misuse Act of 1990) рассматривает как преступление осуществление несанкционированного доступа или вмешательства в компьютерные системы. Наряду с Законом о неправомерном использовании компьютеров (1990 года) [Закон о защите данных 2018 года](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) (Data Protection Act 2018) также охватывает хакерские преступления.

Кроме того, [Закон о следственных полномочиях 2016 года](https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) (Investigatory Powers Act 2016) также криминализирует хакерство и другие виды деятельности, такие как несанкционированный доступ к компьютерным системам.

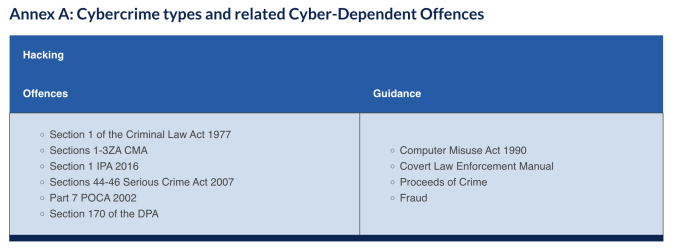
В Великобритании нет специального исключения для «белого» хакерства, однако, если действия осуществляются с разрешения владельца системы и с целью выявления и сообщения об уязвимостях, они не могут считаться незаконными.

В Великобритании предусмотрены три категории наказаний за компьютерный хакерский взлом, каждая из которых имеет разное максимальное наказание:

* Уровень 1 — «несанкционированный доступ к компьютерным материалам», который карается лишением свободы на срок до 2 лет.
* Уровень 2 — «несанкционированный доступ с намерением совершить или способствовать совершению дальнейших преступлений», за который предусмотрено максимальное наказание в виде 5 лет лишения свободы.
* Уровень 3 — «несанкционированные действия с намерением нарушить или по неосторожности нарушить работу компьютера и т. д.», которые могут повлечь за собой тюремное заключение сроком до 10 лет.

Однако в эти правонарушения также были внесены поправки, одна из которых, 3ZA («несанкционированные действия, причиняющие или создающие риск причинения серьезного ущерба»), карается лишением свободы вплоть до пожизненного заключения.

При этом выбор наказания зависит от нескольких различных факторов. Суд будет смотреть, был ли мотив для взлома, например, месть или личная выгода, был ли нанесен какой-либо ущерб лицу или организации, чьи компьютеры были взломаны. Ущерб может включать потерю денег, бизнеса, доверия рынка или последствия доступа к личным или конфиденциальным деловым данным и их использования.



## **ГЕРМАНИЯ**

Взлом (т.е. несанкционированный доступ)

Хакерство является уголовным преступлением в соответствии со статьями 202a и 202b Уголовного кодекса Германии (так называемый «шпионаж данных», статья 202a, и «фишинг» статья 202b). Согласно статье 202a, тот, кто незаконно получает данные для себя или другого лица, которые не предназначались для него и были специально защищены от несанкционированного доступа, если он обошёл защиту, подлежит наказанию в виде лишения свободы на срок до 3 лет или штрафа. Согласно статье 202b, тот, кто, не имея на то полномочий, перехватывает данные, которые не предназначались для него, для себя или другого лица, техническими средствами из непубличной передачи данных или из электромагнитной передачи с объекта обработки данных, подлежит наказанию в виде лишения свободы на срок до 2 лет или штрафа, если преступление не подлежит более суровому наказанию в соответствии с другими положениями. В зависимости от обстоятельств дела «хакерство» может подпадать под определение обоих преступлений, изложенных выше, в зависимости от уровня защиты, применяемого к рассматриваемым данным. Несанкционированный доступ к особо защищенным данным путем преодоления мер безопасности карается тюремным заключением сроком до 3 лет.

Главным камнем преткновения в Германии уже давно является раздел 202c Уголовного кодекса Германии (StGB), который Бундестаг принял в 2007 году вместе с другими статьями о хакерах . Согласно этому разделу, подготовка к уголовному преступлению путем производства, приобретения, продажи, передачи, распространения или предоставления паролей или других кодов безопасности для доступа к данным, а также соответствующих компьютерных программ карается штрафом или тюремным заключением на срок до 1 года. Однако криминализированные таким образом «хакерские инструменты» также используются системными администраторами, программистами и консультантами для проверки сетей и конечных устройств на наличие уязвимостей безопасности.

В ноябре 2023 года министр юстиции Марко Бушманн (СвДП) объявил о реформе статей УК о хакерах, которые были спорными в течение многих лет. Обещали законопроект «в первой половине 2024 года», но этого не произошло.

## **ОАЭ**

Закон № 2 от 2006 года (о киберпреступлениях) ранее предусматривал, что любой, кто совершает преднамеренное действие путем незаконного доступа к электронному сайту, будет наказан тюремным заключением и/или штрафом. Новый закон ОАЭ о киберпреступности (вступил в силу 2 января 2022 года) исключил требование намерения и предусматривает строгие наказания за различные правонарушения, включая взлом, онлайн-мошенничество, кражу личных данных и распространение ложной информации. Наказания варьируются от крупных штрафов до длительного тюремного заключения в зависимости от тяжести преступления. Например, кибератаки на государственные системы или критически важную инфраструктуру могут привести к пожизненному заключению, в то время как незначительные правонарушения, такие как онлайн-клевета, могут повлечь за собой штрафы и более короткие сроки заключения. Закон подчеркивает приверженность ОАЭ защите своей цифровой среды и сдерживанию киберпреступной деятельности.

Несанкционированный доступ к электронному веб-сайту

Согласно ст 4 Нового закона о киберпреступности, несанкционированный доступ к электронному веб-сайту считается серьезным правонарушением. Он подразумевает доступ к веб-сайту или электронной системе без разрешения с целью получения правительственных данных или конфиденциальной информации финансового, торгового или экономического учреждения, что может привести к нецелевому использованию конфиденциальных данных, сбою в работе служб или потенциальным нарушениям безопасности. Наказывается временным лишением свободы и/или штрафом в размере не менее 250 000 дирхамов ОАЭ и не более 1 500 000 дирхамов ОАЭ. Наказание увеличивается, если такие данные изменяются, копируются, удаляются, раскрываются или публикуются, что включает штраф в размере не менее 250 000 дирхамов ОАЭ и не более 1 500 000 дирхамов ОАЭ и/или тюремное заключение на срок не менее 5 лет.

Онлайн-ресурсы для сообщения о киберпреступности:

* Веб -сайт [eCrime](http://www.ecrime.ae/)
* Служба Aman – Полиция Абу-Даби
* Сайт [полиции Дубая](https://www.dubaipolice.gov.ae/wps/portal/home/services/institutionsservices/cybercrimeService/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zi_T29HQ2NvA183U19DQwc3Vwc3U3MXYwNLIz1w1EV-JsFmxg4mhqbuVgYmRsaeJrrRxGj3wAHcDQgrD8KTYm3m6GBo4-niXlYoImBga8hugI0JwYSUgDyA1gBHkcGp-bpF-SGRhhkeuoCAASrB98!/p0/IZ7_P9K01802MGGK30Q8TCLJCD20A2=CZ6_OIKA12K0MG5M00AFDAG47D3083=LA0=Eaction!serviceAction==/#Z7_P9K01802MGGK30Q8TCLJCD20A2)
* Приложение «Мое безопасное общество» было запущено федеральной прокуратурой ОАЭ (приложение доступно в [iTunes](https://itunes.apple.com/ae/app/%D9%85%D8%AC%D8%AA%D9%85%D8%B9%D9%8A-%D8%A2%D9%85%D9%86/id1380618945?mt=8) и [Google Play](https://play.google.com/store/apps/details?id=gov.pp.fio) ).

## **ИЗРАИЛЬ**

К основным израильским законам, применимым к кибербезопасности, относятся Закон Израиля о компьютерах (Israeli Computers Law, 5755-1995), Закон о защите частной жизни, Уголовный кодекс, Закон о контроле за экспортом продукции военного назначения, Закон о регулировании безопасности в государственных органах и (предлагаемая) поправка к Закону об общей службе безопасности.

В Израиле несанкционированный доступ к компьютерам в первую очередь регулируется израильским законом о компьютерах и в некоторой степени также израильским законом о защите конфиденциальности. Израильский закон о компьютерах криминализирует «незаконное проникновение в компьютерные материалы, расположенные в компьютере».

Закон о компьютерах Израиля, 5755-1995 (Israeli Computers Law, 5755-1995), представляет собой закон, который объединяет положения о наказаниях и правонарушениях. Криминализированные деяния включают:

* вмешательство в обычную работу компьютера;
* отрицательно влияющие на целостность компьютеризированного контента;
* передача или хранение мошеннической или вводящей в заблуждение компьютерной информации;
* незаконное вторжение в компьютеры или компьютеризированные материалы;
* разработка, предложение или распространение программного обеспечения, способного выполнить любое из вышеперечисленных действий, или акт вторжения в частную жизнь или незаконное прослушивание телефонных разговоров.

Недавно Верховный суд Израиля постановил, что термин «незаконное проникновение» следует толковать очень широко, как любое использование компьютера без согласия владельца. Суд отверг идею о том, что этот термин следует толковать как охватывающий только случаи проникновения в компьютеры, при котором обходятся технические барьеры доступа. Суд поддержал широкое толкование из-за «… возможного большого ущерба, исходящего от компьютерных преступлений», и отметил, что опасения по поводу чрезмерной криминализации незначительных деяний будут решены, если прокуроры и суды будут использовать исключение de minimis для уголовной ответственности (Руководствуясь доктриной De minimis, суд отказывается рассматривать незначительные дела). Но это никоим образом не означает, что израильские суды, скорее всего, определят, что «взлом хакера» подпадает под исключение de minimis .

## **ПАКИСТАН**

* Electronic Transaction Act (ETO 2002) Закон об электронных транзакциях
* Prevention of Electronic Crime Act «Закон о предотвращении электронных преступлений» 2016 году (PECA 2016)

|  | **Правонарушение** | **Наказание** |
| --- | --- | --- |
| 1 | Создание или загрузка вредоносного кода любым лицом с намерением нанести вред любой [информационной системе](https://www.sciencedirect.com/topics/computer-science/information-system) или повлиять на нее каким-либо образом (разделы 2-3 PECA, 2016) | тюремное заключение сроком до 2-х лет или штраф, или и то, и другое. |
| 2 | Несанкционированный доступ к любой информационной системе (разделом 3, PECA, 2016) | тюремное заключение до 3х месяцев или штраф до 50 000 пакистанских рупий (приблизительно 200 долларов США) |
| 3 | Копирование и/или передача или помощь в передаче любых данных, без разрешения и со злым умыслом | тюремное заключение до 6 месяцев или штраф до 100 000 пакистанских рупий (приблизительно 400 долларов США), лили и то, и другое. |

Закон определяет **«критическую инфраструктуру»** как [критические элементы](https://www.sciencedirect.com/topics/computer-science/critical-element) инфраструктуры, а именно активы, объекты, системы, сети или процессы, потеря или компрометация которых может привести к серьезному пагубному влиянию на доступность, целостность или предоставление основных услуг, включая те услуги, целостность которых, если она будет нарушена, может привести к значительным потерям жизни или жертвам, принимая во внимание значительные экономические или социальные последствия; или влияние на национальную безопасность, национальную оборону или функционирование государства.

В 2021 году с помощью вредоносного кода был осуществлен несанкционированный доступ к данным Федерального налогового управления Пакистана, которые были проданы в даркнете, и это нанесло огромный ущерб Пакистану.

**ВЫВОДЫ:**

1. В Законах при выборе ответственности необходимо делать различия относительно масштаба и направленности воздействия - тогда эффект “ сдерживание” будет работать намного лучше. Наказание создает сдерживание в двух формах: общее (от первого преступления) или специальное (от рецидива).

Общее сдерживание предназначено для непреступников, которые в противном случае были бы готовы совершить преступления, достаточно боясь наказания, чтобы избежать его, воздерживаясь от преступления. Однако специальное сдерживание ограничивает рецидивизм . Сдерживание может иметь место только в той степени, в которой потенциальные преступники ощущают риск наказания. Без этого восприятия не может быть никакого [сдерживающего эффекта](https://www.sciencedirect.com/topics/computer-science/deterrent-effect) .

# **5. Как регламентируются пентесты и баг-баунти государственных структур КИИ - какие требования к верификации хакеров?**

Два метода обнаружения и устранения уязвимостей:

1. **Пентесты** - имитации кибератак, проводимых профессиональными экспертами по безопасности, которые оценивают безопасность системы или сети.
2. **Bug Bounty** - краудсорсинговая инициатива, которая опирается на ИТ специалистов, которые находят и сообщают об уязвимостях или недостатках безопасности в ПО. Вознаграждения только тем, кто успешно находит уязвимости.

| **Критерий** | **Пентест** | **Bug Bounty** |
| --- | --- | --- |
| **Подход** | систематическая запланированная оценка, проводимая профессиональными специалистами по кибербезопасности/белыми хакерами | непрерывная краудсорсинговая модель обнаружения уязвимостей |
| **Временной промежуток** | зафиксированный период на тестирование | непрерывное исследование, в течение времени пока доступна программа |
| **Экспертиза** | в основном проводится сертифицированными профессионалами | Проводится специалистами разного уровня |
| **Конфиденциальность** | высокие требования и уровень конфиденциальности | Зависит от правил платформы, риски выше поскольку доступ имею разные лица |
| **Стоимость** | обычно высокая | Оплата только в случае нахождения уязвимости или ошибки |
| **Отчетность** | детализированный отчет | Описание уязвимости зависит от уровня экспертизы тестировщика, но обычно содержит подробную информацию, которая должна помочь организации понять и воспроизвести проблему |
| **Взаимодействие с заказчиком** | между пентестерами и заказчиком устанавливается личный контакт | нет прямого контакта между пентестером и заказчиком |
| **Какое ПО тестируется** | возможно тестирования неопубликованного ПО | только то, что доступно on-line |

**ТЕНДЕНЦИИ:**

1. Ожидается, что государственное вмешательство в кибербезопасность усилится в ближайшие годы, поскольку киберзащита станет нормативным обязательством во многих секторах.

Например, США стремятся переложить ответственность за кибербезопасность на организации, предоставляющие/производящие продукты и услуги. Аналогичный подход ЕС продвигает в своей Директиве NIS2 и Законе ЕС о киберустойчивости.

1. В последние годы правительства государств создают агентства, призванные защищать КИИ и граждан от киберугроз. Эта задача часто требует разработки новых политик или правил.

# **6. Как законодательно регулируется деятельность баг-баунти платформ? Верифицируют ли платформы хакеров и нужно ли хакером давать о себе полную информацию до выплаты (в момент поиска уязвимости) или везде они действуют анонимно до момента выплаты, как сейчас в РФ?**

Bug Bounty платформы в основном регулируются документами самих платформ.

Но в некоторых странах, разработаны рекомендации. В Сингапуре Агентство кибербезопасности Сингапура (CSA) выпустило рекомендации, Национальный центр кибербезопасности Великобритании (NCSC), в США Министерство юстиции (DOJ) выпустило основу для создания безопасных и надежных программ вознаграждения за обнаружение ошибок (bug bounty) “A Framework for a Vulnerability Disclosure Program for Online Systems”. Программа состоит из 4х шагов:

Шаг 1: Разработать программы раскрытия уязвимостей

• Определить системы и/или данные, которые подпадают под программу.

• Определить, как обрабатывать данные, третьих лиц,

находящихся за пределами организации, включая получение необходимого

разрешения.

• Определить, ограничения на методы и приемы, которые были разрешены для обнаружения уязвимостей.

• Указать типы уязвимостей для целевого использования и как дифференцировать различные типы.

Шаг 2: План администрирования программы раскрытия уязвимостей

• Определить процедуры отчетности и протоколы отправки для решения

проблемы обнаружения уязвимости безопасности.

• Определить контактную точку для получения отчетов об раскрытии уязвимостей.

• Определить персонал, который может помочь с вопросами, касающимися

программы раскрытия уязвимостей организации.

• Решить, как обрабатывать случайные и добросовестные нарушения, а также те, которые являются преднамеренными и злонамеренными.

Шаг 3: Составить политику раскрытия уязвимостей которая точно и недвусмысленно отражает намерение организации

• Определить, какие действия разрешены и запрещены, используя простые, легко понимаемые термины.

• Определить область действия систем и/или данных, которые подпадают под действие программы раскрытия уязвимостей.

• Определить протоколы для работы с ограниченными и конфиденциальными данными, требующими особого обращения.

• Указать последствия за нарушения политик программы раскрытия уязвимостей.

• Поощрять участников получать разъяснения относительно политик программы организации, прежде чем совершать действия, которые могут быть непоследовательными или не охватываться политиками.

Шаг 4: Внедрение программы раскрытия уязвимостей

• Сделать политику программы легкодоступной

• Поощрять участников, которые проводят мероприятия по раскрытию уязвимостей, следуют программе и политикам организации по раскрытию уязвимостей.

• Подготовить отдельное соглашение о сотрудничестве для использования с третьей стороной, содержащее условия участия, соответствующие программе раскрытия уязвимостей и внутренним политикам.

• Установить надлежащие протоколы обучения с определенным набором знаний, ожиданий и механизмов подотчетности, чтобы создать команду информированных сотрудников, которые понимают программу раскрытия уязвимостей организации и ее политики. Эта команда может служить ресурсом для ответов на вопросы и оказания поддержки сторонней службе, чтобы избежать недоразумений и непреднамеренных нарушений.

• Определить, какие правовые или оперативные меры следует предпринять в

случае случайных нарушений, а также преднамеренных. Определите обязательства организации в случае, если внешняя организация инициирует судебный иск против третьей стороны, проводящей оценку безопасности систем организации.

• Подготовить отдельную процедуру отчетности в случае обнаружения уязвимости

**ВЕРИФИКАЦИЯ:**

**ПЕНТЕСТ**

Пентестер известен, заключается договор.

**BUG BOUNTY**

Бывают разные уровни верификации, в зависимости от правил платформы:

1. Частный

Это программа вознаграждения за ошибки, доступная только по приглашению.

1. Публичный

ПО Заказчика, указана на общедоступном сайте, проиндексирована и доступна для поиска в Интернете. Хакеры все равно должны зарегистрироваться на платформе, если они хотят отправить отчет.

1. через Заявку

Хакеры, желающие принять участие в тестировании ПО, должны подать заявку и получить одобрение Заказчика, но все исследователи, зарегистрированные на платформе, могут видеть, что есть это ПО для тестирвания, но подробнотси только после входа в систему и подачи заявки. Если опция «ID-checked» не требуется для исследователей, программа также отображается на общедоступном веб-сайте платформы.

1. через Регистрацию

Все зарегистрированные исследователи на платформе могут видеть полную информацию о ПО и отправлять отчеты. Можно ограничить доступ только для исследователей с проверенным ID.

**Основные проблемы и перспективы рынка Bug Bounty**

* Недостаток доверия: некоторые компании по-прежнему относятся с настороженностью к внешним хакерам, что замедляет развитие рынка.
* Правовые аспекты: важно создать четкую правовую основу для защиты интересов как багхантеров, так и компаний, дав обеим сторонам возможность взаимовыгодного сотрудничества.
* Образование и повышение осведомленности: необходима активная работа по повышению осведомленности о преимуществах программ Bug Bounty среди компаний различного масштаба бизнеса.