



Организационно-правовые основы обеспечения защиты информации в РФ

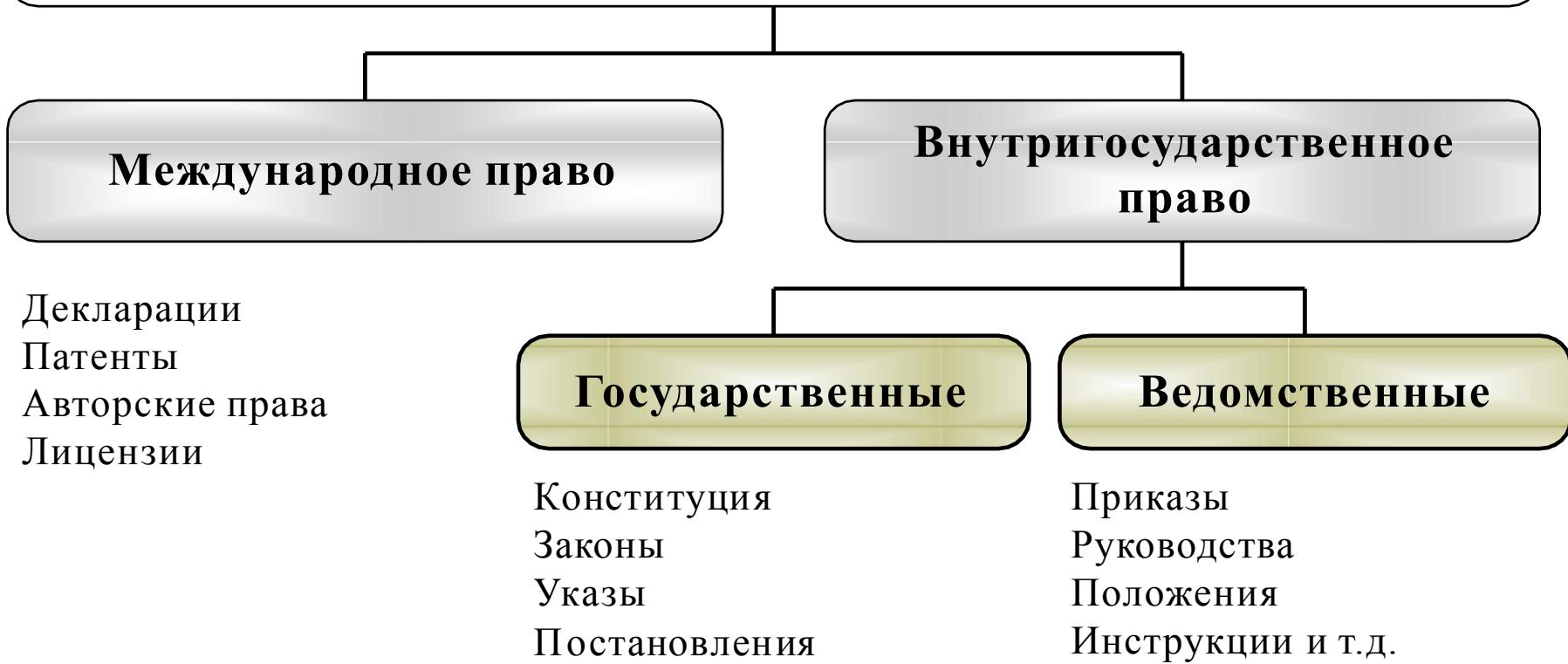
Организационное и правовое
обеспечение ИБ

К.т.н., доцент ИКТИБ ЮФУ
Князева Маргарита Владимировна,
mknnyazeva@sfedu.ru

Структура правовой защиты информации

Правовая защита информации

Специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе



Система документов в области защиты информации

Правовые документы по технической защите информации

Конституция Российской Федерации

Федеральные законы (Законы Российской Федерации)

Указы и распоряжения Президента Российской Федерации

Постановления Правительства Российской Федерации

Организационно-распорядительные документы по технической защите информации

Концепции

Положения

Специальные нормативные документы по технической защите информации

Государственные стандарты

Специальные нормативные документы

Законодательная база обеспечения информационной безопасности

Конституция Российской Федерации

от 12 декабря 1993 г.

Статья 1

1. Российская Федерация - Россия есть демократическое федеративное правовое государство с республиканской формой правления.

Статья 2

Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства.

Статья 4

2. Конституция Российской Федерации и федеральные законы имеют верховенство на всей территории Российской Федерации.
3. Российская Федерация обеспечивает целостность и неприкосновенность своей территории.

Законодательная база обеспечения информационной безопасности

Статья 15

1. Конституция Российской Федерации имеет высшую юридическую силу, прямое действие и применяется на всей территории Российской Федерации. Законы и иные правовые акты, принимаемые в Российской Федерации, не должны противоречить Конституции Российской Федерации.
2. Органы государственной власти, органы местного самоуправления, должностные лица, граждане и их объединения обязаны соблюдать Конституцию Российской Федерации и законы.
3. Законы подлежат официальному опубликованию. Неопубликованные законы не применяются. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения.
4. Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора.

Законодательная база обеспечения информационной безопасности

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.
2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 29

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.
5. Гарантируется свобода массовой информации. Цензура запрещается.

Стратегия национальной безопасности РФ

Утверждена Указом Президента РФ от 31 декабря 2015 г. № 683

Настоящая Стратегия является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу.

Стратегия призвана консолидировать усилия федеральных органов государственной власти, других государственных органов, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, институтов гражданского общества по созданию благоприятных внутренних и внешних условий для реализации национальных интересов и стратегических национальных приоритетов Российской Федерации.

Стратегия национальной безопасности РФ

II. Россия в современном мире

Государственная политика в сфере обеспечения национальной безопасности и социально-экономического развития Российской Федерации способствует реализации стратегических национальных приоритетов и эффективной защите национальных интересов. В настоящее время создана устойчивая основа для дальнейшего наращивания экономического, политического, военного и духовного потенциалов Российской Федерации, повышения ее роли в формирующемся полиглобальном мире.

Для предотвращения угроз национальной безопасности Российская Федерация сосредоточивает усилия на укреплении внутреннего единства российского общества, обеспечении социальной стабильности, межнационального согласия и религиозной терпимости, устраниении структурных дисбалансов в экономике и ее модернизации, повышении обороноспособности страны.

Стратегия национальной безопасности РФ

III. Национальные интересы и стратегические национальные приоритеты

Национальными интересами на долгосрочную перспективу являются:

- укрепление обороны страны, обеспечение незыблемости конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации;
- укрепление национального согласия, политической и социальной стабильности, развитие демократических институтов, совершенствование механизмов взаимодействия государства и гражданского общества;
- повышение качества жизни, укрепление здоровья населения, обеспечение стабильного демографического развития страны;
- сохранение и развитие культуры, традиционных российских духовно-нравственных ценностей;
- повышение конкурентоспособности национальной экономики;
- закрепление за Российской Федерацией статуса одной из лидирующих мировых держав, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях полигонетического мира.

Стратегия национальной безопасности РФ

IV. Обеспечение национальной безопасности

Состояние национальной безопасности напрямую зависит от степени реализации стратегических национальных приоритетов и эффективности функционирования системы обеспечения национальной безопасности.

Основные положения военной политики и задачи военно-экономического обеспечения обороны страны, военные опасности и военные угрозы определяются Военной доктриной Российской Федерации.

V. Организационные, нормативно-правовые и информационные основы реализации настоящей Стратегии

При реализации настоящей **Стратегии** особое внимание уделяется обеспечению **информационной безопасности** с учетом стратегических национальных приоритетов.

Информационная и информационно-аналитическая поддержка реализации настоящей Стратегии, ее корректировка, проводимая один раз в шесть лет с учетом результатов мониторинга ее реализации и изменений, оказывающих существенное влияние на состояние национальной безопасности, осуществляются при координирующей роли Совета Безопасности Российской Федерации.

Доктрина информационной безопасности РФ

Утверждена Указом Президента РФ от 5 декабря 2016 г. № 646

Информационная безопасность Российской Федерации
(информационная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Угроза информационной безопасности Российской Федерации
(информационная угроза) - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Доктрина информационной безопасности РФ

Утверждена Указом Президента РФ от 5 декабря 2016 г. № 646

Обеспечение информационной безопасности - осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Силы обеспечения информационной безопасности - государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности.

Доктрина информационной безопасности РФ

Утверждена Указом Президента РФ от 5 декабря 2016 г. № 646

Средства обеспечения информационной безопасности - правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности.

Система обеспечения информационной безопасности - совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

Информационная инфраструктура Российской Федерации - (информационная инфраструктура) совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

Доктрина информационной безопасности РФ

Утверждена Указом Президента РФ от 5 декабря 2016 г. № 646

II. Национальные интересы в информационной сфере

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

Национальными интересами в информационной сфере являются:

- а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий ...;
- б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации...;
- в) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;
- г) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий

Основные федеральные законы в области защиты информации

«О безопасности»	Федеральный закон РФ от 28 декабря 2010 г. №390-ФЗ
«О государственной тайне»	Федеральный закон РФ от 21 июля 1993 г. №5485-1
«О коммерческой тайне»	Федеральный закон РФ от 29 июля 2004 г. №98-ФЗ
«О техническом регулировании»	Федеральный закон РФ от 27 декабря 2002 г. №184-ФЗ
«О лицензировании отдельных видов деятельности»	Федеральный закон РФ от 4 мая 2011 г. №99-ФЗ
«Об электронной подписи»	Федеральный закон РФ от 6 апреля 2011 г. №63-ФЗ
«Об информации, информационных технологиях и о защите информации»	Федеральный закон РФ от 27 июля 2006 г. №149-ФЗ
«О персональных данных»	Федеральный закон РФ от 27 июля 2006 г. №152-ФЗ
КоАП РФ	Федеральный закон от 30 декабря 2001 г. №195-ФЗ
УК РФ	Федеральный закон от 13 июня 1996 г. №63

Основные федеральные законы в области защиты информации

Закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-1

Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Определяет основные понятия, полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты.

Дает перечень сведений, которые могут быть отнесены к государственной тайне.

Указывает принципы засекречивания сведений, перечисляет сведения, не подлежащие засекречиванию.

Устанавливает степени секретности сведений и грифы секретности носителей этих сведений.

Термины и определения

государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

система защиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;

доступ к сведениям, составляющим государственную тайну, - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Сведения, составляющие государственную тайну

Перечень сведений, составляющих государственную тайну (ст.5) - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

- Сведения в военной области:

-
-
-

- Сведения в области экономики, науки и техники:

-
-
-

- Сведения в области внешней политики и экономики:

-
-
-

- Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

-
- о методах и средствах защиты секретной информации;
- об организации и о фактическом состоянии защиты государственной тайны;

-

Степень секретности

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ вследствие распространения указанных сведений.

Гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

особой важности

совершенно секретно

секретно

Сведения, не подлежащие отнесению к государственной тайне

Сведения, не подлежащие отнесению к государственной тайне (ст.7)

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах Российской Федерации;
- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суде.

Основные федеральные законы в области защиты информации

Федеральный закон «О безопасности»

28 декабря 2010 года № 390-ФЗ

определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством РФ, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления в области безопасности, а также статус Совета Безопасности РФ.

Основные принципы обеспечения безопасности (ст.2)

- 1) соблюдение и защита прав и свобод человека и гражданина;
- 2) законность;
- 3) системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;
- 4) приоритет предупредительных мер в целях обеспечения безопасности;
- 5) взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Деятельность по обеспечению безопасности включает в себя (ст.3):

- 1) прогнозирование, выявление, анализ и оценку угроз безопасности;
- 2) определение основных направлений государственной политики и стратегическое планирование в области обеспечения безопасности;
- 3) правовое регулирование в области обеспечения безопасности;
- 4) разработку и применение комплекса оперативных и долговременных мер по выявлению, предупреждению и устраниению угроз безопасности, локализации и нейтрализации последствий их проявления;
- 5) применение специальных экономических мер в целях обеспечения безопасности;
- 6) разработку, производство и внедрение современных видов вооружения, военной и специальной техники, а также техники двойного и гражданского назначения в целях обеспечения безопасности;
- 7) организацию научной деятельности в области обеспечения безопасности;
- 8) координацию деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области обеспечения безопасности;
- 9) финансирование расходов на обеспечение безопасности, контроль за целевым расходованием выделенных средств;
- 10) международное сотрудничество в целях обеспечения безопасности;
- 11) осуществление других мероприятий в области обеспечения безопасности в соответствии с законодательством Российской Федерации.

Основные федеральные законы в области защиты информации

ФЗ «О техническом регулировании»
от 27 декабря 2002 г. № 184-ФЗ

Регулирует отношения, возникающие при:

- разработке, принятии, применении и исполнении обязательных требований к продукции, к процессам проектирования, производства, эксплуатации, хранения, перевозки, реализации и утилизации;
- разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, ...эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг в целях добровольного подтверждения соответствия;
- оценке соответствия.

Определяет права и обязанности участников регулируемых настоящим Федеральным законом отношений.

Термины и определения

Безопасность продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации (далее - безопасность) - состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений;

Декларирование соответствия - форма подтверждения соответствия продукции требованиям технических регламентов;

Декларация о соответствии - документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов

Заявитель - физическое или юридическое лицо, которое для подтверждения соответствия принимает декларацию о соответствии или обращается за получением сертификата соответствия, получает сертификат соответствия;

Термины и определения

Международный стандарт - стандарт, принятый международной организацией;

Орган по сертификации - юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации;

Оценка соответствия - прямое или косвенное определение соблюдения требований, предъявляемых к объекту;

Подтверждение соответствия - документальное удостоверение соответствия продукции или иных объектов, процессов ... требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

Риск - вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда;

Основные федеральные законы в области защиты информации

ФЗ «О лицензировании отдельных видов деятельности»

от 4 мая 2011 г. № 99-ФЗ

Лицензирование отдельных видов деятельности осуществляется в целях предотвращения ущерба правам, законным интересам, жизни или здоровью граждан, окружающей среде, объектам культурного наследия (памятникам истории и культуры) народов Российской Федерации, обороне и безопасности государства, возможность нанесения которого связана с осуществлением юридическими лицами и индивидуальными предпринимателями отдельных видов деятельности.

Осуществление лицензирования отдельных видов деятельности в иных целях не допускается.

Термины и определения

Лицензирование - деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования;

Лицензия - специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в форме электронного документа;

Термины и определения

Лицензирующие органы - уполномоченные федеральные органы исполнительной власти и (или) их территориальные органы, а в случае передачи осуществления полномочий Российской Федерации в области лицензирования органам государственной власти субъектов Российской Федерации органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование;

Соискатель лицензии - юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии;

Лицензиат - юридическое лицо или индивидуальный предприниматель, имеющие лицензию;

Лицензионные требования - совокупность требований, которые установлены положениями о лицензировании конкретных видов деятельности, основаны на соответствующих требованиях законодательства Российской Федерации и направлены на обеспечение достижения целей лицензирования;

Основные федеральные законы в области защиты информации

ФЗ “Об информации, информационных технологиях и о защите информации”
от 27 июля 2006 года №149-ФЗ

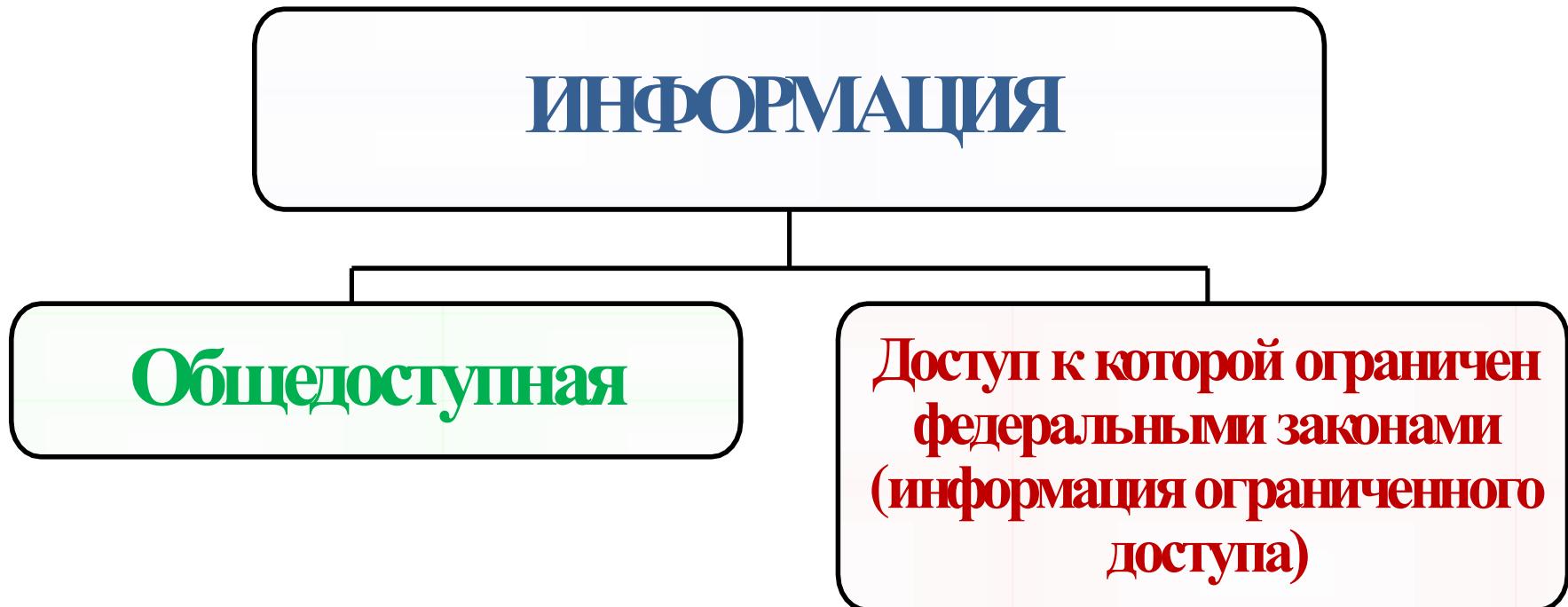
Регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
 - применении информационных технологий и обеспечении защиты информации.
-
- **информация** - сведения (сообщения, данные) независимо от формы их представления;
 - **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
 - **доступ к информации** - возможность получения информации и ее использования.

Классификация информации по категории доступа

- Информация может являться объектом публичных, гражданских и иных правовых отношений.
- Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Классификация информации по категории доступа



Классификация информации в зависимости от порядка ее предоставления/распространения

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Классификация информации в зависимости от порядка её предоставления или распространения

ИНФОРМАЦИЯ

Информация, свободно распространяемая

Информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях

Информация, распространение которой в РФ ограничивается или запрещается

Информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению

Права и обязанности обладателя информации

Обладатель информации (ст.6)

Права:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обязанности:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Права физических лиц и организаций

Граждане (физические лица) и организации (юридические лица) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

Не может быть ограничен доступ к: (ст.8)

- 1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- 2) информации о состоянии окружающей среды;
- 3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- 4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
- 5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Конвенция Совета Европы О защите физических лиц при автоматизированной обработке персональных данных

Цель обеспечение прав и основных свобод человека на неприкосновенность частной жизни и особенно в связи с автоматической обработкой касающихся его персональных данных.

Персональные данные - информация, касающаяся конкретного или могущего быть идентифицированным лица ("субъекта данных").

*Страсбург, 28 января 1981
изменения от 15 июня 1999
подписана Россией 8 ноября 2001
вступила в силу 1 октября 1985*

ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»

№ 160-ФЗ от 19 декабря 2005 г.

Основные федеральные законы в области защиты информации

ФЗ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ

Регулирует отношения, связанные с обработкой персональных данных, осуществляющей федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, . . . физическими лицами с использованием средств автоматизации или без использования таких средств, . . .

Целью настоящего ФЗ является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Основные федеральные законы в области защиты информации

Персональные данные - любая информация, относящаяся к определенному или определяемому физическому лицу (субъекту персональных данных), в том числе:

- фамилия
- имя
- отчество
- год
- месяц
- дата и место рождения
- адрес
- профессия
- другая информация

ФЗ «О персональных данных»

от 27 июля 2006 г. № 152-ФЗ

Ст.3. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая:

- сбор
- запись
- систематизацию
- накопление
- хранение
- уточнение (обновление, изменение)
- извлечение
- использование
- передачу (распространение, предоставление, доступ),
- Обезличивание
- Блокирование
- Удаление
- уничтожение персональных данных;

ФЗ «О персональных данных»
от 27 июля 2006 г. № 152-ФЗ

Конфиденциальность персональных данных. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

ФЗ «О персональных данных»
от 27 июля 2006 г. № 152-ФЗ

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Общедоступные персональные данные. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

Основные федеральные законы в области защиты информации

ФЗ РФ «О коммерческой тайне» № 98-ФЗ от 29.07.2004 г.

Настоящий Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Основные федеральные законы в области защиты информации

ФЗ РФ «О коммерческой тайне» № 98-ФЗ от 29.07.2004 г.

Информация, составляющая коммерческую тайну (секрет производства), - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Основные федеральные законы в области защиты информации

ФЗ РФ «О коммерческой тайне» № 98-ФЗ от 29.07.2004 г.

Обладатель информации, составляющей коммерческую тайну - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайне.

Доступ к информации, составляющей коммерческую тайну - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Контрагент - сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

Основные федеральные законы в области защиты информации

ФЗ РФ «О коммерческой тайне» № 98-ФЗ от 29.07.2004 г.

- **Предоставление информации, составляющей коммерческую тайну**, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.
- **Разглашение информации, составляющей коммерческую тайну** - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, или иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Основные федеральные законы в области защиты информации

ФЗ РФ «О коммерческой тайне» № 98-ФЗ от 29.07.2004 г.

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.

Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

Охрана конфиденциальности информации (ст. 10)

Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Охрана конфиденциальности информации (ст.10)

Наряду с мерами, указанными выше, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

Меры по охране конфиденциальности информации признаются **разумно достаточными**, если:

- исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;
- обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Предоставление информации, составляющей коммерческую тайну (ст.6)

Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию обязаны предоставить эту информацию по запросу судов, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

Предоставление информации, составляющей коммерческую тайну (ст.6)

На документах, предоставляемых указанным органам государственной власти и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф "Коммерческая тайна" с указанием ее обладателя (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Ответственность за нарушение Федерального закона

1. Нарушение настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.
2. Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

Ответственность за нарушение Федерального закона

3. Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.

4. Лицо, которое использовало информацию, составляющую коммерческую тайну, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с настоящим Федеральным законом быть привлечено к ответственности.

5. По требованию обладателя информации, составляющей коммерческую тайну, лицо, указанное в части 4 настоящей статьи, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав.

Сведения, которые не могут составлять коммерческую тайну

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- 1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- 2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- 3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- 4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

Сведения, которые не могут составлять коммерческую тайну

- 5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;
- 6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- 7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
- 8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- 9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
- 10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- 11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Основные федеральные законы в области защиты информации

Федеральный закон Российской Федерации "Об электронной подписи"
№ 63-ФЗ от 6 апреля 2011 г.

Регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Основные понятия, используемые в настоящем Федеральном законе

1) электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

2) сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Основные федеральные законы в области защиты информации

Федеральный закон Российской Федерации "Об электронной подписи"
№ 63-ФЗ от 6 апреля 2011 г.

Основные понятия, используемые в настоящем Федеральном законе

3) **квалифицированный сертификат ключа проверки электронной подписи** (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

4) **владелец сертификата ключа проверки электронной подписи** - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки

Основные понятия, используемые в Федеральном законе «О персональных данных»

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;

Удостоверяющий центр - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

Аkkредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

Основные понятия, используемые в Федеральном законе «О персональных данных»

Средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

Корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

Информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано;

Вручение сертификата ключа проверки электронной подписи - передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу;

Подтверждение владения ключом электронной подписи - получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

Виды электронных подписей



Виды электронных подписей

Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Неквалифицированной электронной подписью является электронная подпись, которая:

- 1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- 2) позволяет определить лицо, подпавшее электронный документ;
- 3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- 4) создается с использованием средств электронной подписи.

Виды электронных подписей

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- 1) ключ проверки электронной подписи указан в квалифицированном сертификате;
- 2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Указы Президента РФ

Указ Президента РФ «Вопросы Федеральной службы по техническому и экспортному контролю» от 16 августа 2004 г. № 1085 (ред. от 31.08.2020 г.)
Вводит в действие Положение «О Федеральной службе по техническому и экспортному контролю» в котором определяются полномочия и организация деятельности
ФСТЭК.

Указ Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 года № 1203 (с изм. на 23.07.2020 г.)

В соответствии со статьей 4 Закона РФ «О государственной тайне» **утверждается** перечень сведений, отнесенных к государственной тайне.

Правительству РФ предписывается организовать работу по приведению действующих нормативных актов в соответствие с Перечнем сведений, отнесенных к государственной тайне.

Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188

утверждает перечень сведений конфиденциального характера:

- 1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.**
- 2. Сведения, составляющие тайну следствия и судопроизводства.**
- 3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).**

Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188

утверждает перечень сведений конфиденциального характера:

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.
7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц.

**Указ Президента РФ «О мерах по обеспечению информационной безопасности
Российской Федерации при использовании информационно-
телекоммуникационных сетей международного информационного обмена»
от 17 марта 2008 г. № 351**

В целях обеспечения информационной безопасности РФ при использовании информационно-телекоммуникационных сетей (И-ТС), позволяющих осуществлять передачу информации через гос. границу РФ, в том числе при использовании международной компьютерной сети "Интернет", постановляет:

- а) подключение информационных систем (ИС), И-ТС и средств вычислительной техники (СВТ), применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие гос. тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к И-ТС, позволяющим осуществлять передачу информации через государственную границу РФ, в том числе к международной компьютерной сети "Интернет" **не допускается**;
- б) при необходимости подключения ИС, И-ТС и СВТ, указанных в подпункте "а" настоящего пункта, к И-ТС международного информационного обмена (МИО) такое подключение производится только с использованием специально предназначенных для этого средств защиты информации (СЗИ), в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством РФ порядке сертификацию в ФСБ РФ и (или) получивших подтверждение соответствия в ФСТЭК. Выполнение данного требования является обязательным для операторов ИС, владельцев И-ТС и (или) СВТ;

Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 г. № 351

- в) государственные органы в целях защиты общедоступной информации, размещаемой в ИТС МИО, используют только СЗИ, прошедшие в установленном законодательством РФ порядке сертификацию в ФСБ РФ и (или) получившие подтверждение соответствия в ФСТЭК;
- г) размещение технических средств, подключаемых к И-ТС МИО, содержащие сведения, составляющие гос.тайну, осуществляется только при наличии сертификата, разрешающего эксплуатацию таких технических средств в указанных помещениях. Финансирование расходов, связанных с размещением технических средств в указанных помещениях федеральных органов гос. власти, осуществляется в пределах бюджетных ассигнований, предусмотренных в федеральном бюджете на содержание этих органов.

Постановления Правительства РФ

Постановление Правительства РФ «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» от 3 ноября 1994 г. № 1233

Постановление Правительства РФ «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств...» от 16 апреля 2012 г. № 313

Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119

Положения по защите информации

<p>Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны</p>	<p>Утверждено постановлением Правительства Российской Федерации от 15 апреля 1995 года № 333 (с изменениями и дополнениями от 23.08.2018 г. № 984)</p>
<p>Положение о лицензировании деятельности по технической защите конфиденциальной информации</p>	<p>Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (с изменениями и дополнениями от 15.06.2016 № 541)</p>
<p>Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации</p>	<p>Утверждено постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171 (с изменениями и дополнениями от 10.07.2020 № 1017)</p>

**Постановление Правительства РФ «Об утверждении Положения об
обеспечении безопасности персональных данных при их обработке в
информационных системах персональных данных»
от 01.11.2012 № 1119**

- 1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных.**
- 2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных".**

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных".

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

5. Информационная система является информационной системой, обрабатывающей **специальные категории персональных данных**, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей **биометрические персональные данные**, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

Информационная система является информационной системой, обрабатывающей **общедоступные персональные данные**, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей **иные категории персональных данных**, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей **персональные данные сотрудников оператора**, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

6. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".
8. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.
9. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:
 - а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;
 - б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

10. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;
- б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;
- г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

11. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;
- д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

12. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;
- б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

- а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- б) обеспечение сохранности носителей персональных данных;
- в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119

16. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 настоящего документа, необходимо выполнение следующих требований:

- а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;
- б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

17. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации» от 15 сентября 2008 г. № 687 г.

В целях реализации ФЗ "О персональных данных" Правительство РФ постановляет:

1. Утвердить прилагаемое Положение об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации.
2. Федеральным органам исполнительной власти в месячный срок привести свои акты по вопросам обработки персональных данных, осуществляющейся без использования средств автоматизации, в соответствие с настоящим постановлением.
3. Настоящее постановление вступает в силу по истечении одного месяца со дня его официального опубликования.

Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации» от 15 сентября 2008 г. № 687 г.

- I. Общие положения.
 - II. Особенности организации обработки персональных данных, осуществляющейся без использования средств автоматизации.
 - III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляющейся без использования средств автоматизации
13. Обработка персональных данных, осуществляющаяся без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
14. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
15. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Приказы ФСТЭК

Об утверждении административного регламента федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации	Приказ федеральной службы по техническому и экспортному контролю от 17 июля 2017 г. № 134 (в ред. Приказа ФСТЭК России от 17.12.2019 № 240)
Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации	Приказ федеральной службы по техническому и экспортному контролю от 12 июля 2012 г. № 84 (в ред. Приказа ФСТЭК России от 11.02.2013 N 15)
Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации	Приказ федеральной службы по техническому и экспортному контролю от 20 июля 2012 г. № 89 (с изм. на 21.12.2016 г.)
Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации	Приказ федеральной службы по техническому и экспортному контролю от 12 июля 2012 г. № 90 (с изм. На 12.12.2019 г.)

Приказы ФСБ

Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по осуществлению федерального государственного контроля за обеспечением защиты государственной тайны	Приказ ФСБ России от 05 марта 2015 года № 152
Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по осуществлению лицензионного контроля деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)	Приказ ФСБ России от 23 марта 2016 г. № 182
Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по осуществлению лицензионного контроля деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации	Приказ ФСБ России от 23 марта 2016 г. № 183
Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по осуществлению лицензионного контроля деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)	Приказ ФСБ России от 23 марта 2016 г. № 184
Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по осуществлению лицензионного контроля деятельности по разработке и производству средств защиты конфиденциальной информации	Приказ ФСБ России от 23 марта 2016 г. № 185

Акты Президента РФ

О Стратегии национальной безопасности Российской Федерации	Указ Президента Российской Федерации от 31 декабря 2015 года № 683
Об утверждении Доктрины информационной безопасности Российской Федерации	Указ Президента Российской Федерации от 5 декабря 2016 года № 646
О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы	Указ Президента Российской Федерации от 9 мая 2017 г. N 203
Вопросы Федеральной службы по техническому и экспортному контролю	Указ Президента Российской Федерации от 16 августа 2004 года № 1085 (с изм. на 31 августа 2020 г.)
Вопросы Межведомственной комиссии по защите государственной тайны	Указ Президента Российской Федерации № 1286 (с изм. на 3 августа 2018 г.)
Об утверждении Перечня сведений, отнесенных к государственной тайне	Указ Президента Российской Федерации от 1995 года № 1203 (с изменениями на 23 июля 2020 г.)
Об утверждении Перечня должностных лиц органов государственной власти Российской Федерации, наделенных полномочиями по отнесению сведений к государственной тайне	Распоряжение Президента Российской Федерации от 16 апреля 2005 г. № 151-рп
Об утверждении Перечня сведений конфиденциального характера	Указ Президента Российской Федерации от 1997 года № 188 (с изм. на 13 июля 2015 г.)
О межведомственном коллегиальном органе - коллегии Федеральной Службы по Техническому и Экспортному Контролю	Распоряжение Президента Российской Федерации от 29 декабря 2008 г. № 821-рп
О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена	Указ Президента РФ от 22 мая 2015 г. № 260
О реестре должностей федеральной государственной гражданской службы	Указ Президента Российской Федерации от 2005 г. № 1574 (с изм. на 30 июля 2020 г.)

Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ

Статья 13.11. Нарушение законодательства РФ в области персональных данных

- предупреждение
- на граждан в размере от 700 до 3000 рублей;
- для должностных лиц от 4000 до 10 000 рублей;
- для индивидуальных предпринимателей от 10 000 до 20 000 рублей;
- для юридических лиц от 20 000 до 50 000 рублей.

Статья 13.12. Нарушение правил защиты информации.

Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну).

- на граждан в размере от 1 000 до 1 500 рублей;
- на должностных лиц - от 1 500 до 2 500 рублей;
- на юридических лиц - от 15 000 до 20 000 рублей.

Кодекс Российской Федерации об административных правонарушениях
от 30 декабря 2001 г. № 195-ФЗ

Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну).

Административный штраф:

- на граждан в размере от **1 500** до **2 500** рублей с конфискацией несертифицированных средств защиты информации или без таковой;
- на должностных лиц - от **2 500** до **3 000** рублей;
- на юридических лиц - от **20 000** до **25 000** рублей с конфискацией несертифицированных средств защиты информации или без таковой.

Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ

Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей ГТ, созданием средств, предназначенных для ЗИ, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей ГТ.

- **Административный штраф:**
 - на должностных лиц в размере от **2 000** до **3 000** рублей;
 - на юридических лиц - от **20 000** до **25 000** рублей.

Использование несертифицированных средств, предназначенных для ЗИ, составляющей ГТ.

- **Административный штраф:**
 - на должностных лиц в размере от **3 000** до **4 000** рублей;
 - на юридических лиц - от **20 000** до **30 000** рублей с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ

Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну)

Административный штраф

- на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица от **2 000** до **3 000** рублей или административное приостановление деятельности на срок до девяноста суток;
- на должностных лиц - от **2 000** до **3 000** рублей;
- на юридических лиц - от **20 000** до **25 000** рублей или административное приостановление деятельности на срок до девяноста суток.

Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ

Статья 13.13. Незаконная деятельность в области защиты информации.

Занятие видами деятельности в области ЗИ (за исключением информации, составляющей ГТ) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна).

Административный штраф:

- на граждан в размере от **500** до **1 000** рублей с конфискацией средств защиты информации или без таковой;
- на должностных лиц - от **2 000** до **3 000** рублей с конфискацией средств защиты информации или без таковой;
- на юридических лиц - от **10 000** до **20 000** рублей с конфискацией средств защиты информации или без таковой.

Кодекс Российской Федерации об административных правонарушениях
от 30 декабря 2001 г. № 195-ФЗ

Занятие видами деятельности, связанной с использованием и ЗИ, составляющей ГТ, созданием средств, предназначенных для ЗИ, составляющей ГТ, осуществлением мероприятий и (или) оказанием услуг по ЗИ, составляющей ГТ без лицензии.

Административный штраф:

- на должностных лиц в размере от **4 000** до **5 000** рублей;
- на юридических лиц - от **30 000** до **40 000** рублей с конфискацией созданных без лицензии средств защиты информации, составляющей ГТ, или без таковой.

Кодекс Российской Федерации об административных правонарушениях
от 30 декабря 2001 г. № 195-ФЗ

Статья 13.14. Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

Административный штраф:

- на граждан в размере от **500** до **1 000** рублей;
- на должностное лицо - от **4 000** до **5 000** рублей.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 137. Нарушение неприкосновенности частной жизни

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации:

- штраф в размере до **200 000** рублей или в размере заработной платы или иного дохода осужденного за период до **18** месяцев,
- либо обязательные работы на срок до **360** часов,
- либо исправительные работы на срок до **1** года,
- либо принудительными работами на срок до **2** лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо арестом на срок до **4** месяцев, либо лишением свободы на срок до **2** лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

2. Те же деяния, совершенные лицом с использованием своего служебного положения:

- штраф в размере от **100 000** до **300 000** рублей или в размере заработной платы или иного дохода осужденного за период от одного года до **2** лет,
- либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок до **5** лет,
- либо арест на срок до **6** месяцев,
- либо лишением свободы на срок до **4** лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан:

- штраф в размере до **80 000** рублей, или в размере заработной платы или иного дохода осужденного за период до **6** месяцев,
- либо обязательные работы на срок от **120** до **180** часов,
- либо исправительные работы на срок до **1** года.

Уголовный кодекс Российской Федерации

от 13 июня 1996 года № 63-ФЗ

- 2. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации:
 - штраф в размере от **100 000** до **300 000** рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет,
 - либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок от **2** до **5** лет,
 - либо обязательные работы на срок до **480** часов,
 - либо арест на срок до **4** месяцев.
 - либо лишением свободы на срок до **4** лет.
- Незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации:
 - штраф в размере до **200 000** рублей или в размере заработной платы или иного дохода осужденного за период до **18** месяцев,
 - либо ограничение свободы на срок до **4** лет...
 - либо лишение свободы на срок до **4** лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до **3** лет.

Уголовный кодекс Российской Федерации

Понятие и цели наказания. Виды наказаний.

- **Обязательные работы** выполнение осужденным в свободное от основной работы или учебы время бесплатных общественно полезных работ. Вид обязательных работ и объекты, на которых они отбываются, определяются органами местного самоуправления по согласованию с уголовно-исполнительными инспекциями.
- **Исправительные работы** назначаются осужденному, не имеющему основного места работы, и отбываются в местах, определяемых органом местного самоуправления по согласованию с органом, исполняющим наказания в виде исправительных работ, но в районе места жительства осужденного.
- **Ограничение свободы** заключается в установлении судом осужденному следующих ограничений: не уходить из места постоянного проживания (пребывания) в определенное время суток, не посещать определенные места, расположенные в пределах территории соответствующего муниципального образования, не выезжать за пределы территории соответствующего муниципального образования, не посещать места проведения массовых и иных мероприятий и не участвовать в указанных мероприятиях, не изменять место жительства или пребывания, место работы и (или) учебы без согласия специализированного государственного органа, осуществляющего надзор за отбыванием осужденными наказания в виде ограничения свободы, в случаях, предусмотренных законодательством Российской Федерации.

Уголовный кодекс Российской Федерации
от 13 июня 1996 года № 63-ФЗ

Понятие и цели наказания. Виды наказаний.

- **Арест** заключается в содержании осужденного в условиях строгой изоляции от общества и устанавливается на срок от одного до шести месяцев. В случае замены обязательных работ или исправительных работ арестом он может быть назначен на срок менее одного месяца.
- **Лишение свободы** заключается в изоляции осужденного от общества путем направления его в колонию-поселение, помещения в воспитательную колонию, лечебное исправительное учреждение, исправительную колонию общего, строгого или особого режима либо в тюрьму.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 146. Нарушение авторских и смежных прав

1. Присвоение авторства (плагиат), если это деяние причинило крупный ущерб автору или иному правообладателю, -

наказывается штрафом в размере до 200 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок до 480 часов, либо арестом на срок до 6 месяцев.

2. Незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере, -

наказываются штрафом в размере до 200 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок до 480 часов, либо исправительными работами на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы до 2 лет.

Уголовный кодекс Российской Федерации
от 13 июня 1996 года № 63-ФЗ

Статья 146. Нарушение авторских и смежных прав

3. Деяния, предусмотренные частью второй настоящей статьи, если они совершены:

группой лиц по предварительному сговору или организованной группой;

в особо крупном размере;

лицом с использованием своего служебного положения, -

наказываются принудительными работами на срок до 5 лет, либо лишением свободы на срок до 6 лет со штрафом в размере до 500 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до 3 лет либо без такового.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом:

- штраф в размере до **500 000** тысяч рублей или в размере заработной платы или иного дохода осужденного за период до **1** года,
- либо исправительными работами на срок до одного года, либо принудительными работами на срок до **2** лет, либо лишением свободы на тот же срок .

Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе:

- штраф в размере до **1 000 000** рублей или в размере заработной платы или иного дохода осужденного за период до **2** лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до **3** лет,
- либо исправительными работами на срок до **2** лет, либо принудительными работами на срок до **3** лет, либо лишением свободы на тот же срок.

Уголовный кодекс Российской Федерации
от 13 июня 1996 года № 63-ФЗ

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности:

- штраф в размере до 1 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет,
- либо принудительными работами на срок до 5 лет, либо лишением свободы на тот же срок.

Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия:

...лишением свободы на срок до 7 лет.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 272. Неправомерный доступ к компьютерной информации.

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации , -

- наказывается штрафом в размере до **200 000 рублей** или в размере заработной платы или иного дохода осужденного за период до **18 месяцев**,
- либо исправительными работами на срок до **1 года**,
- либо ограничением свободы на срок до **2 лет**,
- либо принудительными работами на срок до **2 лет**, либо лишением свободы на тот же срок

То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

- наказывается штрафом в размере от **100 000** до **300 000** рублей или в размере заработной платы или иного дохода осужденного за период от **1 года** до **2 лет**,
- либо исправительными работами на срок от **1 года** до **2 лет**,
- либо ограничением свободы на срок до **4 лет**,
- либо принудительными работами на срок до **4 лет**,
- либо лишением свободы на тот же срок.

Уголовный кодекс Российской Федерации
от 13 июня 1996 года № 63-ФЗ

Статья 272. Неправомерный доступ к компьютерной информации.

Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -

- наказывается штрафом в размере до **500 000 рублей** или в размере заработной платы или иного дохода осужденного за период до **3 лет**, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до **3 лет**,
- либо ограничением свободы на срок до **4 лет**,
- либо принудительными работами на срок до **5 лет**,
- либо лишением свободы на тот же срок.

Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до **7 лет.**

Уголовный кодекс Российской Федерации
от 13 июня 1996 года № 63-ФЗ

Статья 272. Неправомерный доступ к компьютерной информации.

- 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.**

- 2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает 1 000 000 рублей.**

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

- наказываются ограничением свободы на срок до четырех лет,
- либо принудительными работами на срок до четырех лет,
- либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

- наказываются ограничением свободы на срок до четырех лет,
- либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового,
- либо лишением свободы на срок до 5 лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Уголовный кодекс Российской Федерации
от 13 июня 1996 года № 63-ФЗ

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Уголовный кодекс Российской Федерации
от 13 июня 1996 года № 63-ФЗ

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и окончного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -

- наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев,
- либо исправительными работами на срок от шести месяцев до одного года,
- либо ограничением свободы на срок до двух лет,
- либо принудительными работами на срок **до 2 лет**,
- либо лишением свободы на тот же срок.

Уголовный кодекс Российской Федерации
от 13 июня 1996 года № 63-ФЗ

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, - наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, -
наказываются

- принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового
- либо лишением свободы на срок от двух до пяти лет со штрафом в размере от 500000 до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации, -

- наказывается принудительными работами на срок до пяти лет со штрафом в размере от 500 тыс. до 1 млн. рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового
- либо лишением свободы на срок от двух до шести лет со штрафом в размере от 500 тыс. до 1 млн. рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

Уголовный кодекс Российской Федерации

от 13 июня 1996 года № 63-ФЗ

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, ... , если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, -

наказывается

- принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового
- либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 275. Государственная измена.

Государственная измена, то есть совершенные гражданином Российской Федерации шпионаж, выдача иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, доверенную лицу или ставшую известной ему по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации, либо оказание финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности Российской Федерации, - наказывается

лишением свободы на срок от двенадцати до двадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 276. Шпионаж.

Передача, собирание, похищение или хранение в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки или лица, действующего в ее интересах, иных сведений для использования их против безопасности Российской Федерации, то есть шпионаж, если эти деяния совершены иностранным гражданином или лицом без гражданства, - наказываются лишением свободы на срок от десяти до двадцати лет.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 283. Разглашение государственной тайны.

Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации, если эти сведения стали достоянием других лиц -

наказывается

- арестом на срок от четырех до шести месяцев
- либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
- То же деяние, повлекшее по неосторожности тяжкие последствия,
 -
- наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ

Статья 284. Утрата документов, содержащих государственную тайну.

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, - наказывается

- ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев,
- либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Системный подход к управлению безопасностью:

Законодательный уровень

Административный уровень

Процедурный уровень

Технический уровень



Лекция 1

К.т.н., доцент ИКТИБ ЮФУ

Князева Маргарита Владимировна

Иерархия средств защиты от информационных угроз

Законодательный уровень

Правовое регулирование, стандартизация, лицензирование, законы.

Участниками правоотношений являются **субъекты правоотношений**, к которым в области ИБ можно отнести:

- А) Обладателей информации
- Б) Потребителей информации
- В) Операторов ИС
- Г) Владельцев сайтов в сети Интернет
- Д) Провайдеров телекоммуникационных сетей
- Е) Разработчиков программных и аппаратных средств информационных технологий

Права и обязанности субъектов правоотношений определяются по отношению к **объектам правоотношений**:

- 1) Информационным системам
- 2) СЗИ и криптографическим системам
- 3) Услугам в области ИБ
- 4) Информация (составляющая государственную, коммерческую, банковскую, семейную тайны)
- 5) Персональным данным

Административный уровень

Процедурный уровень

Технический уровень

Обзор нормативно-правовых актов РФ в области информационной безопасности

Общегосударственная система мер по обеспечению ИБ России базируется на *Доктрине РФ, утвержденной Президентом РФ 9 сентября, 2000 г.*

В соответствие с Доктриной защита информации включает:

- А) защиту информации и права на нее, включая право на тайну. Права на интеллектуальную собственность, право на доступ к информации;
- Б) защиту информационных систем и прав на них;
- В) защиту от вредоносной информации.

Федеральный закон «Об информации, информационных технологиях и о защите информации»: №149 ФЗ от 8 июля 2006г.

Статья 1: Настоящий Федеральный закон регулирует отношения, возникающие при:

- 1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
- 2) применении информационных технологий;
- 3) обеспечении защиты информации.

Федеральный закон «Об информации, информационных технологиях и о защите информации»: №149 ФЗ от 8 июля 2006г.

Статья 2: Основные понятия, используемые в настоящем Федеральном законе:

- 1) **информация** - сведения (сообщения, данные) независимо от формы их представления;
- 2) **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- 3) **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- 4) **информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- 5) **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- 6) **доступ к информации** - возможность получения информации и ее использования;
- 7) **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- 8) **предоставление информации** - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
- 9) **распространение информации** - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
- 10) **электронное сообщение** - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
- 11) **документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- 12) **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Федеральный закон «Об информации, информационных технологиях и о защите информации»: №149 ФЗ от 8 июля 2006г.

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- 1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- 2) установление ограничений доступа к информации только федеральными законами;
- 3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами (Тендеры, Гранты, Закупки, Выборы);
- 4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- 5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 6) достоверность информации и своевременность ее предоставления;
- 7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Федеральный закон «Об информации, информационных технологиях и о защите информации»: 149 ФЗ от 8 июля 2006г.

Статья 7. Общедоступная информация

1. К общедоступной информации относятся общезвестные сведения и иная информация, доступ к которой не ограничен.
**Дополнение к этой статье устанавливает, что «Информация, размещаемая ее обладателями в сети "Интернет" в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных.*
(часть 4 введена Федеральным законом от 07.06.2013 N 112-ФЗ)».
2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.
3. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

«Пакет Яровой» состоит из двух законопроектов:

№ 1039101-6 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» (№ 375-ФЗ от 6 июля 2016 г.)

№ 1039149-6 «О внесении изменений в отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»[26] (№ 374-ФЗ от 6 июля 2016 г.)

Хранение интернет-трафика

Второй законопроект обязывает операторов связи хранить звонки и сообщения абонентов за период, определяемый Правительством Российской Федерации (но не более, чем за 6 месяцев) в соответствии с 64-й статьей федерального закона «О связи», а информацию о фактах приема, передачи, доставки и обработки сообщений и звонков — 3 года.

Согласно проекту приказа Минкомсвязи, интернет-компании и сервисы должны хранить и предоставлять спецслужбам: псевдоним, дату рождения, адрес, фамилию, имя, отчество, паспортные данные, языки, которыми владеет пользователь, список его родственников, текст сообщений, аудио- и видеозаписи, адрес электронной почты, дату и время авторизации и выхода из информационного сервиса, наименование программы-клиента.

12 апреля 2018 года правительство РФ подписало постановление о том, что с 1 октября 2018 года операторы связи обязаны хранить в течение 30 суток текстовые, голосовые, видео- и другие сообщения пользователей. Далее оператор обязан увеличивать объем хранения на 15 процентов в год.

Средства шифрования

Законопроект устанавливает запрет на использование несертифицированных средств кодирования (шифрования). За нарушение этого запрета нарушителю грозит штраф в размере от 3 000 до 5 000 руб. с конфискацией средств шифрования. Также «закон Яровой» обязывает организаторов распространения информации в интернете декодировать сообщения пользователей. По требованию ФСБ компании должны будут предоставлять ключи к зашифрованному трафику.

Федеральный закон «Об информации, информационных технологиях и о защите информации»: №149 ФЗ от 8 июля 2006г.

Статья 9. Ограничение доступа к информации

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.
3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.
4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.
5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.
6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.
7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.
8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.
9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Федеральный закон «Об информации, информационных технологиях и о защите информации»: 149 ФЗ от 8 июля 2006г.

Статья 11. Документирование информации

1. Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.
2. В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.
3. Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается *электронным документом, равнозначным документу, подписанному собственноручной подписью*, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

Статья 15. Использование информационно-телекоммуникационных сетей

Статья 15.1. Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено (введена Федеральным законом от 28.07.2012 N 139-ФЗ).

В целях ограничения доступа к сайтам в сети "Интернет", содержащим информацию, распространение которой в Российской Федерации запрещено, создается единая автоматизированная информационная система "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено"

Федеральный закон «Об информации, информационных технологиях и о защите информации»: 149 ФЗ от 8 июля 2006г.

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модификации, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- 2) соблюдение конфиденциальности информации ограниченного доступа,
- 3) реализацию права на доступ к информации.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- 1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- 2) своевременное обнаружение фактов несанкционированного доступа к информации;
- 3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- 4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- 6) постоянный контроль за обеспечением уровня защищенности информации.

Уголовный кодекс РФ

Статья 138 УК РФ. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года. (в ред. Федеральных законов от 08.12.2003 N 162-ФЗ, от 07.12.2011 N 420-ФЗ)

Статья 183 УК РФ. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

1. *Сбор сведений*, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом - наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. *Незаконные разглашение или использование сведений*, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, -

наказываются штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок.

Уголовный кодекс РФ

ГЛАВА 28 УК РФ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -
наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -
наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -
наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (введена Федеральным законом от 26.07.2017 N 194-ФЗ)

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, -
наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

Критическая информационная инфраструктура Российской Федерации

Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

безопасность критической информационной инфраструктуры (КИИ) - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

значимый объект критической информационной инфраструктуры - объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

субъекты критической информационной инфраструктуры - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

***ГосСОПКА** (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак) создаётся для обмена информацией о кибератаках на информационные системы КИИ. Указ Президента Российской Федерации от 15 января 2013 г. N 31c г. Москва "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации"

Законы и нормативно-правовые акты

Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 20.07.2020) "О национальной платежной системе"

Статья 27. Обеспечение защиты информации в платежной системе. (Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, поставщики платежных приложений, операторы платежных систем, операторы услуг платежной инфраструктуры обязаны обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации.

Правительство Российской Федерации устанавливает требования к защите указанной информации.)

Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

- Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
- Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- Обработка подлежат только персональные данные, которые отвечают целям их обработки.
- Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частями 2 и 2.1 настоящей статьи.

Постановление Правительства Российской Федерации от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных". (для гос. и муницип. органов).

Приказ ФСТЭК России от 11 февраля 2013 г. N 17 ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙNU, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ.

Настоящие Требования являются обязательными при обработке информации в государственных информационных системах, функционирующих на территории Российской Федерации, а также в муниципальных информационных системах. Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый).

Устанавливаются три класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс - третий, самый высокий - первый. Класс защищенности информационной системы определяется в соответствии с приложением N 1 к настоящим Требованиям. (в ред. Приказа ФСТЭК России от 15.02.2017 N 27).

Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ

Иерархия средств защиты от информационных угроз

Законодательный уровень

Административный уровень

Политика информационной безопасности (организационно-технические и режимные меры).

Политика информационной безопасности — набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области ЗИ. На основе ПИБ строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение ИС в различных ситуациях.

Для конкретной ИС политика безопасности должна быть индивидуальной. Она зависит от технологии обработки информации, используемых программных и технических средств, структуры организации и т.д.

Следует рассматривать такие направления защиты ИС:

- 01 Защита объектов информационной системы;
- 02 Защита процессов, процедур и программ обработки информации;
- 03 Защита каналов связи;
- 04 Подавление побочных электромагнитных излучений;
- 05 Управление системой защиты.

Процедурный уровень

Технический уровень

Принципы политики безопасности

Политика безопасности (ГОСТ 50922-2006) определяется как совокупность документированных управленческих решений, правил, процедур, руководящих принципов, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

1. Невозможность миновать защитные средства;
2. Усиление самого слабого звена;
3. Недопустимость перехода в открытое состояние;
4. Минимизация привилегий;
5. Разделение обязанностей;
6. Многоуровневая эшелонированная защита;
7. Разнообразие защитных средств;
8. Простота и управляемость информационной системы;
9. Обеспечение всеобщей поддержки мер безопасности.

Виды политик безопасности:

- Избирательная политика безопасности (дискреционное, избирательное управление доступом);
- Полномочная политика безопасности (мандатное управление доступом);

Организационно-технические мероприятия

Приведем перечень основных организационно-технические мероприятия по ЗИ:

- разработка и утверждение функциональных обязанностей должностных лиц службы информационной безопасности;
- внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, обязанности должностных лиц, инструкции пользователей системы и т.п.) по вопросам обеспечения безопасности программно-информационных ресурсов ИС и действиям в случае возникновения кризисных ситуаций;
- оформление юридических документов (договора, приказы и распоряжения руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в автоматизированной системе, между участниками информационного обмена и третьей стороной (арбитраж, третейский суд) о правилах разрешения споров, связанных с применением электронной подписи;
- определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы; правил управления доступом к ресурсам системы;
- определение перечня файлов и баз данных, содержащих сведения, составляющие коммерческую и служебную тайну, а также требования к уровням их защищенности от НСД при передаче, хранении и обработке в ИС;
- выявление наиболее вероятных угроз для данной ИС, выявление уязвимых мест процесса обработки информации и каналов доступа к ней;
- оценка возможного ущерба, вызванного нарушением безопасности информации, разработка адекватных требований по основным направлениям защиты;
- определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;
- организация учета, хранения, использования и уничтожения документов и носителей с закрытой информацией; определение перечня необходимых мер по обеспечению непрерывной работы ИС в критических ситуациях, возникающих в результате НСД, сбоев и отказов СВТ, ошибок в программах и действиях персонала, стихийных бедствий и т.п.
- контроль функционирования и управление используемыми средствами защиты;
- контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования ИС; периодический анализ состояния и оценка эффективности мер защиты информации;

Уровни политики безопасности

Верхний уровень

К верхнему уровню относятся решения, затрагивающие организацию в целом. Они носят общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- формирование или пересмотр комплексной программы обеспечения информационной безопасности, определение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей; обеспечение базы для соблюдения законов и правил;
- формулировка управленческих решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Цели политики верхнего уровня организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности.

Если организация ответственна за поддержание критически важных баз данных, на первом плане может стоять уменьшение случаев потерь, повреждений или искажений данных.

Средний уровень

К среднему уровню следует отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией. Примеры таких вопросов — отношение к передовым, но недостаточно проверенным технологиям: доступ к Internet (как сочетать свободу получения информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Нижний уровень

Политика безопасности нижнего уровня касается конкретных сервисов. Она включает в себя два аспекта — цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем детальнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими мерами.

Описание позиции организации

Целью организации является обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности. Более частными целями являются:

- обеспечение уровня безопасности, соответствующего нормативным документам;
- следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности);
- обеспечение безопасности в каждой функциональной области локальной сети;
- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;
- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;
- обеспечение соответствия действующим законам и общеорганизационной политике безопасности.
- Выделение области действия политик, ролей и обязанностей пользователей.

Главная цель мер, предпринимаемых на управленческом уровне, — сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Периодическая переоценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

Краткое содержание документов

“Концепция обеспечения информационной безопасности в ИС” содержит:

- общую характеристику объекта защиты (описание состава, функций и существующей технологии обработки данных в типовой ИС);
- формулировку целей создания системы защиты, основных задач обеспечения информационной безопасности и путей достижения целей (решения задач);
- перечень типичных угроз информационной безопасности и возможных путей их реализации, неформальная модель вероятных нарушителей;
- основные принципы и подходы к построению системы обеспечения информационной безопасности, меры, методы и средства достижения целей защиты.

“План защиты” от несанкционированного доступа к информации и незаконного вмешательства в процесс функционирования ИС содержит:

- ❖ определение целей, задач защиты информации в ИС и основных путей их достижения (решения);
- ❖ требования к организации и проведению работ по защите информации в ИС;
- ❖ описание применяемых мер и средств защиты информации от рассматриваемых угроз, общих требований к настройкам применяемых средств защиты информации от НСД;
- ❖ распределение ответственности за реализацию “Плана защиты ИС” между должностными лицами и структурными подразделениями организации.

Краткое содержание документов

“Положение о категорировании ресурсов ИС” содержит:

- формулировку целей введения классификации ресурсов (АРМ, задач, информации, каналов передачи) по степеням (категориям) защищенности;
- предложения по числу и названиям категорий защищаемых ресурсов и критериям классификации ресурсов по требуемым степеням защищенности (категориям);
- определение мер и средств защиты информации, обязательных и рекомендуемых к применению на АРМ различных категорий;
- общие положения, специальные термины и определения, встречающиеся в документе;
- образец формуляра ЭВМ (для учета требуемой степени защищенности (категории), комплектации, конфигурации и перечня решаемых на ЭВМ задач);
- образец формуляра решаемых на ЭВМ ИС функциональных задач (для учета их характеристик, категорий пользователей задач и их прав доступа к информационным ресурсам данных задач).

Краткое содержание документов

“Порядок обращения с информацией, подлежащей защите” содержит:

- ✓ определение основных видов защищаемых (конфиденциальных) сведений (информационных ресурсов);
- ✓ общие вопросы организации учета, хранения и уничтожения документов и магнитных носителей конфиденциальной информации;
- ✓ порядок передачи (предоставления) конфиденциальных сведений третьим лицам;
- ✓ определение ответственности за нарушение установленных правил обращения с защищаемой информацией;
- ✓ форму типового Соглашения (обязательства) сотрудника организации о соблюдении требований обращения с защищаемой информацией.

“План обеспечения непрерывной работы и восстановления” включает:

- общие положения (назначение документа);
- классификацию возможных (значимых) кризисных ситуаций и указание источников получения информации о возникновении кризисной ситуации;
- перечень основных мер и средств обеспечения непрерывности процесса функционирования ИС и своевременности восстановления ее работоспособности;
- общие требования к подсистеме обеспечения непрерывной работы и восстановления;
- типовые формы для планирования резервирования ресурсов подсистем ИС и определения конкретных мер и средств обеспечения их непрерывной работы и восстановления;
- порядок действий и обязанности персонала по обеспечению непрерывной работы и восстановлению работоспособности системы.



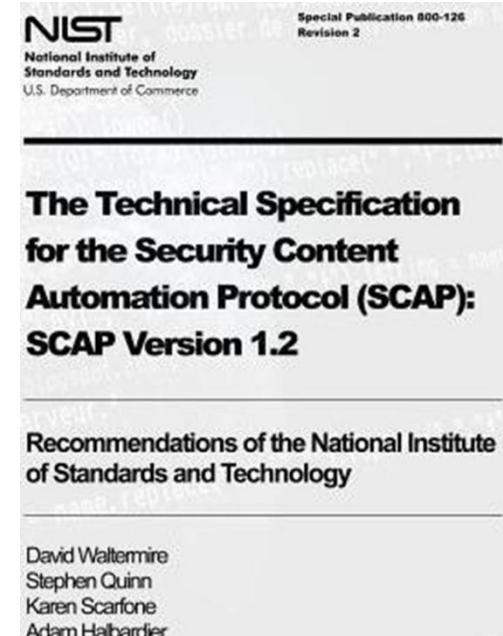
Международный
союз
электросвязи

МСЭ-Т X.1200-X.1500 СЕКТОР СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ Х: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

К.т.н., доцент ИКТИБ ЮФУ

Князева Маргарита Владимировна



РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X
СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589

СЕРИЯ Х: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

Х.1205 Обзор кибербезопасности

Кибербезопасность – это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя.

Ресурсы организации и пользователя включают подсоединеные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде.

Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде.

Модели безопасности: CIA, STRIDE

Общие задачи обеспечения безопасности включают следующее:

- доступность;
- целостность, которая может включать аутентичность и неотказуемость;
- конфиденциальность.

Кибербезопасность и риски ИБ

Этот процесс включает в себя задачу идентификации совокупного набора компонентов, которые нужно защитить:

1) Нарушение защиты в виде прерывания обслуживания.

Этот тип взлома отключает доступ пользователя к намеченным услугам временно или постоянно. Примерами являются: потеря доступа к сайту во всемирной сети, неспособность провести финансовую операцию или инициировать речевой вызов. Несколько типов взломов могут привести к нарушению обслуживания. Например, "отказ в обслуживании" (DoS), "распределённый отказ в обслуживании" (DDoS) или разрушение зданий, в которых размещается важная инфраструктура, может привести к препятствию для доступа пользователей к услуге.

2) Несанкционированный доступ к активам.

Эти типы взломов включают в себя кражу или неправильное использование инфраструктуры. Взломы этого типа могут существенно повлиять на кибербезопасность, если они проводятся в большом масштабе.

3) Захват компонентов.

Эти типы взломов включают в себя захват контроля над некоторыми устройствами, а затем использование их для запуска новых взломов, направленных против других компонентов киберсреды.

Угрозы кибербезопасности: подходы

Согласно Рекомендации МСЭ-Т Х.800, в перечень угроз для системы передачи данных включены

следующие:

- a) уничтожение информации и/или других ресурсов;
- b) искажение или изменение информации;
- c) кража, перемещение или потеря информации и/или других ресурсов;
- d) раскрытие информации; и
- e) прерывание обслуживания.

Анализ угроз, анализ уязвимости (включая оценку воздействия), меры противодействия и механизмы обеспечения безопасности:

- a) идентификация уязвимых мест системы;
- b) анализ вероятности угроз, нацеленных на использование этих уязвимых мест;
- c) оценка последствий, если каждая угроза будет успешно выполнена;
- d) оценка стоимости каждой попытки нарушения защиты;
- e) расчет стоимости потенциальных мер противодействия; и
- f) выбор механизмов безопасности, которые оправданы (возможно с помощью использования анализа стоимостной выгоды).

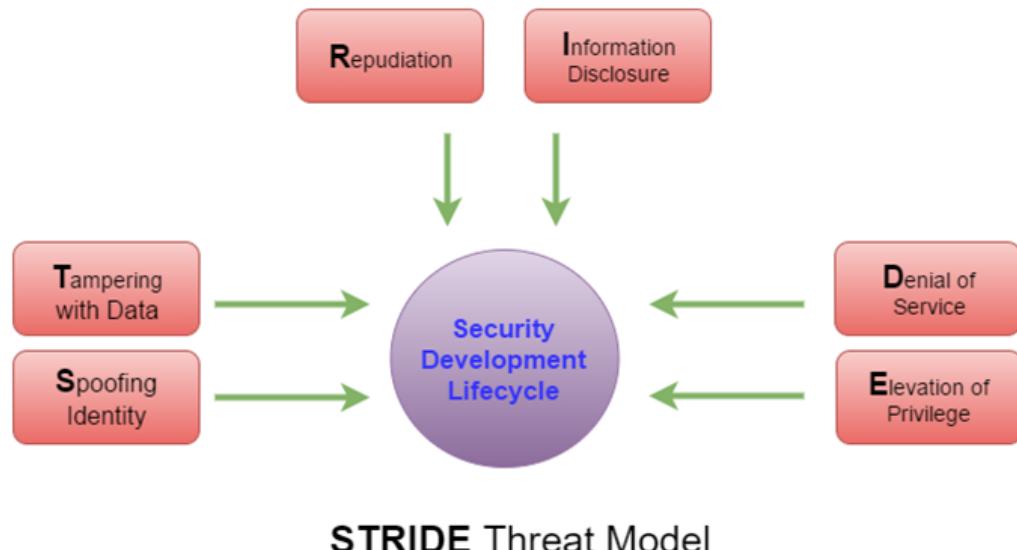
Факторы безопасности

В [ITU-T X.805] фактором безопасности является совокупность мер безопасности, разработанных для определенного аспекта безопасности сетей.

В [ITU-T X.805] определяется восемь факторов, которые защищают от всех основных угроз безопасности. Эти факторы не ограничиваются сетями, а также распространяются на приложения и информацию конечного пользователя. Эти факторы безопасности применимы для поставщиков услуг или предприятий, предлагающих услуги безопасности своим потребителям.

Факторами безопасности являются:

- 1) контроль доступа;
- 2) аутентификация;
- 3) неотказуемость;
- 4) конфиденциальность данных;
- 5) безопасность связи;
- 6) целостность данных;
- 7) готовность; и
- 8) секретность.

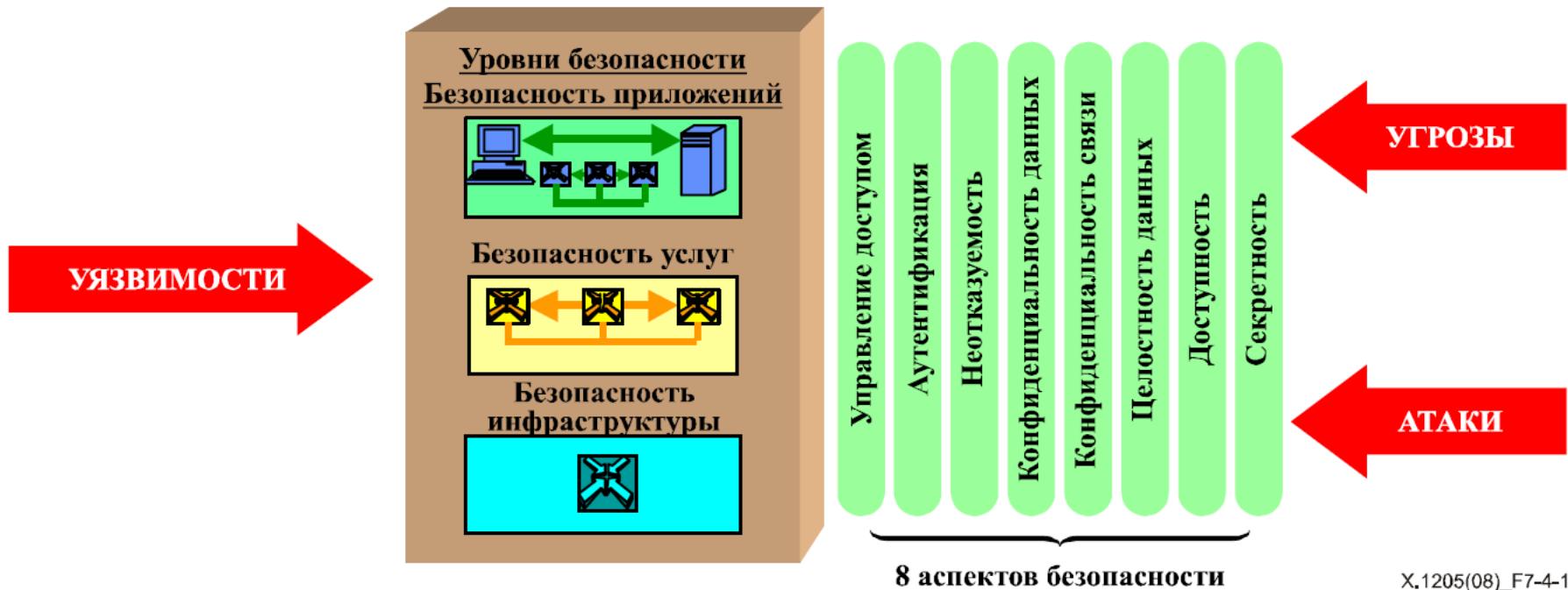


Для того чтобы обеспечить решение вопроса сквозной безопасности связи факторы безопасности должны применяться к иерархии сетевого оборудования и группировкам средств, которые рассматриваются, как уровни безопасности.

Обращаются к трем следующим уровням:

- 1) уровень безопасности инфраструктуры;
- 2) уровень безопасности услуг; и
- 3) уровень безопасности приложений.

Факторы безопасности



В [ITU-T X.805] плоскость безопасности это определенный тип действия сети, защищенный с помощью факторов безопасности. В [ITU-T X.805] определено три плоскости безопасности для представления трех типов защищенных действий, которые происходят в сети. Плоскостями безопасности являются:

- 1) плоскость управления;
- 2) плоскость контроля; и
- 3) плоскость конечного пользователя.



МСЭ-Т X.1500 (04/2011)

СЕКТОР СТАНДАРТИЗАЦИИ

ЭЛЕКТРОСВЯЗИ МСЭ

**СЕРИЯ Х: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ.**

Обмен информацией, касающейся
кибербезопасности – Обзор кибербезопасности
Методы обмена информацией
о кибербезопасности.

Обзор кибербезопасности X.1500–X.1519

Обмен информацией об уязвимости/состоянии X.1520–X.1539

Обмен информацией о событии/инциденте/эвристических правилах X.1540–X.1549

Обмен информацией о политике X.1550–X.1559

Эвристические правила и запрос информации X.1560–X.1569

Идентификация и обнаружение X.1570–X.1579

Гарантированный обмен X.1580–X.1589

МСЭ-Т Х.1500 (04/2011): CYBEX

СЕРИЯ Х: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ.

Обмен информацией, касающейся
кибербезопасности – Обзор кибербезопасности.
Методы обмена информацией
о кибербезопасности.



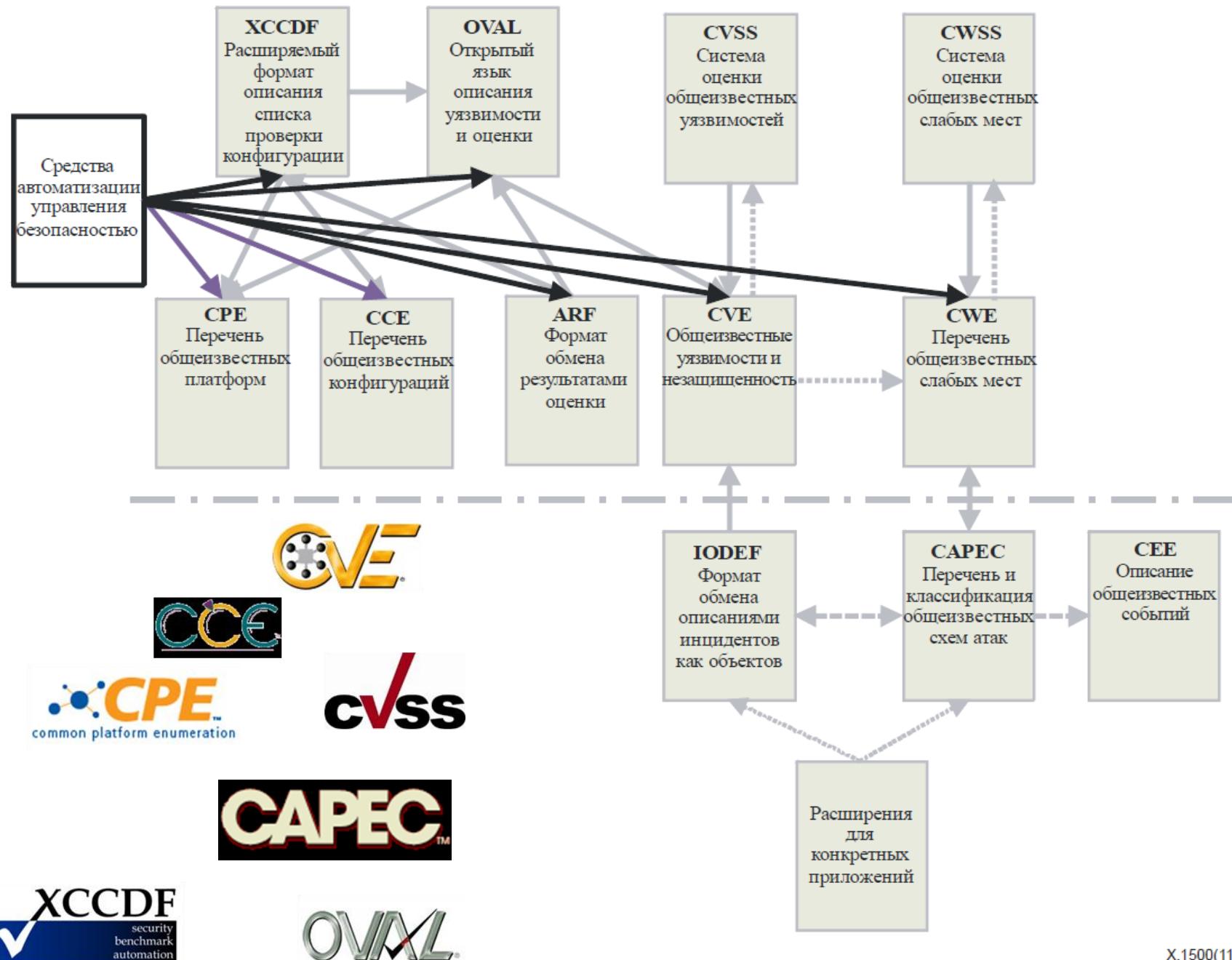
Настоящая Рекомендация, касающаяся обмена информацией о кибербезопасности (CYBEX - Cybersecurity Information Exchange Techniques), призвана выполнить простую конкретную задачу – описать методы, с помощью которых объекты кибербезопасности могут обмениваться информацией о кибербезопасности с использованием методов, обеспечивающих достаточный уровень гарантии:

- а) *Структурирование информации о кибербезопасности для целей обмена.*
- б) *Идентификация и обнаружение информации о кибербезопасности и объектов кибербезопасности.*
- в) *Заключение соглашения о доверии и политике между объектами, осуществляющими обмен.*
- г) *Запрашивание и предоставление информации о кибербезопасности.*
- д) *Гарантирование целостности обмена информацией о кибербезопасности.*

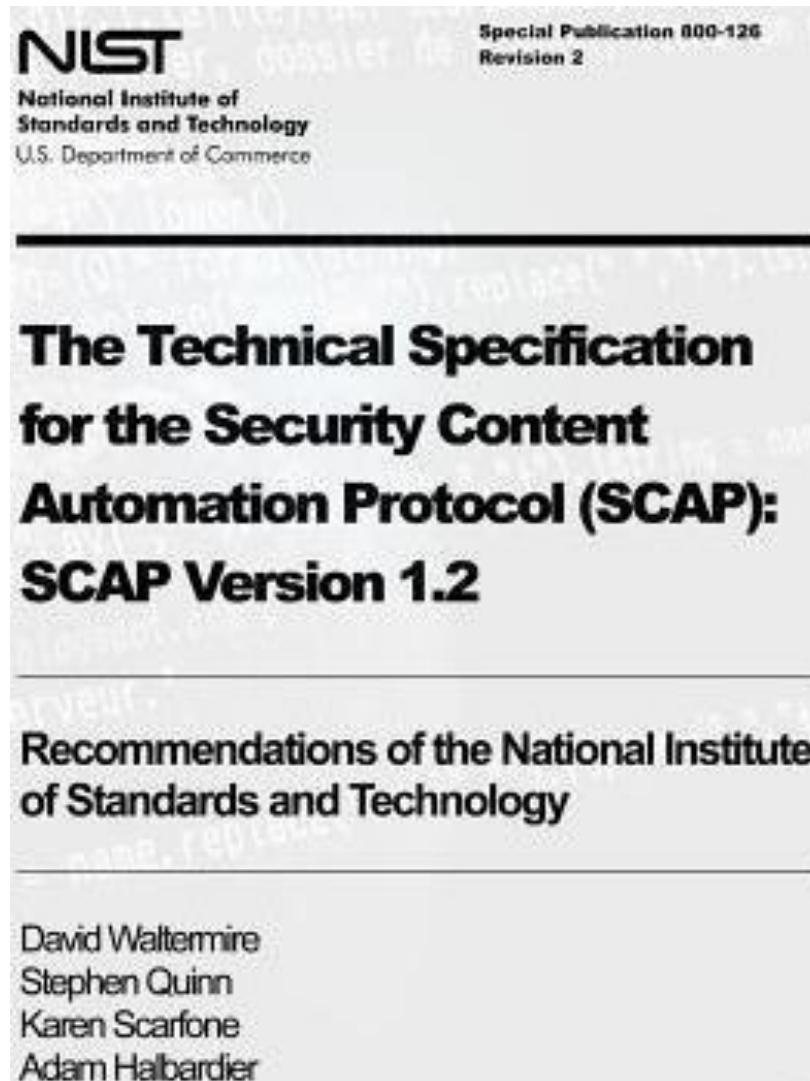
С тем чтобы описать на общем уровне желательные атрибуты обмена информацией о кибербезопасности, средства структурированной информации сгруппированы по следующим шести блокам методов, относящихся к отдельным группам обмена информацией о кибербезопасности:

- слабые места, уязвимость и состояние;
- событие, инцидент и эвристика;
- политика обмена информацией;
- идентификация, обнаружение и запрос;
- гарантия идентичности;
- протокол обмена.





The Security Content Automation Protocol (SCAP)



Стандарты SCAP (The Security Content Automation Protocol). Протокол автоматизации управления данными безопасности

Протокол автоматизации управления данными безопасности (SCAP) представляет собой набор открытых стандартов, определяющих технические спецификации для представления и обмена данными по безопасности. Эти данные могут быть использованы для автоматизации процесса поиска уязвимостей, оценки соответствия технических механизмов контроля и измерения уровня защищенности.

SCAP (Security Content Automation Protocol) включает в себя ряд открытых стандартов, поддерживаемых международным сообществом профессионалов в области информационной безопасности. Последняя версия SCAP состоит из одиннадцати компонентов протокола в пяти категориях:

- 1. Языки.** Языки SCAP стандартизуют словари и выражения, описывающие политику безопасности, механизмы контроля и результаты оценки. SCAP включает в себя следующие компоненты:
Расширяемый формат описания контрольного списка конфигураций (XCCDF, Extensible configuration checklist description format);
Открытый язык описания уязвимостей и проведения оценок (OVAL, Open vulnerability and assessment language);
Открытый интерактивный язык описания контрольного списка (OCIL, Open checklist interactive language).

Стандарты SCAP (The Security Content Automation Protocol).

- 1. Языки.** Языки SCAP стандартизуют словари и выражения, описывающие политику безопасности, механизмы контроля и результаты оценки. SCAP включает в себя следующие компоненты:
Расширяемый формат описания контрольного списка конфигураций (XCCDF, Extensible configuration checklist description format);
Открытый язык описания уязвимостей и проведения оценок (OVAL, Open vulnerability and assessment language);
Открытый интерактивный язык описания контрольного списка (OCIL, Open checklist interactive language).
- 2. Формат отчетов.** Форматы отчета SCAP представляют необходимые конструкции, для выражения собранной информации в стандартизованных форматах:
Формат представления данных об активах ИБ (Asset Reporting Format);
Формат для уникальной идентификации активов ИБ на основе идентификаторов (Asset Identification [AI]).
- 3. Перечни.** Перечни SCAP определяют стандартизованные спецификации, официальные перечни (словари), выраженные с использованием этих спецификаций. SCAP включает в себя следующие перечни:
Общий перечень платформ (CPE , Common platform enumeration);
Общий перечень конфигураций (CCE , Common configuration enumeration);
Общий перечень уязвимостей и рисков (CVE, Common vulnerabilities and exposures).
- 4. Измерение и оценка систем.** В SCAP это выражается в оценке определенных особенностей уязвимости (например, слабых мест программного обеспечения и проблем конфигурации безопасности) и определении количественного значения влияния уязвимости (метрики). Метрики SCAP в терминах системных технических требований описываются
Общей системой оценки уязвимости (CVSS, Common vulnerability scoring system) и
Общей системой оценки конфигурации (CCSS, Common configuration scoring system).
- 5. Целостность.** Спецификация целостности SCAP предназначена для обеспечения целостности информационного SCAP-контента и полученных с помощью него результатов. Модель доверия для данных об автоматизации безопасности (TMSAD, Trust Model for Security Automation Data) является спецификацией целостности SCAP.

СЕРИЯ Х: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

Обмен информацией, касающейся
кибербезопасности – Обмен информацией
об уязвимости/состоянии

<https://www.itu.int/rec/T-REC/en>



X.1520 (01/2014) Общеизвестные уязвимости и незащищенность.

В Рекомендации МСЭ-Т X.1520 об использовании общеизвестных уязвимостях и незащищенности (CVE) предлагается структурированное средство обмена информацией об уязвимостях и незащищенности в области безопасности, обеспечивающее общие названия широко известных проблем в коммерческом программном обеспечении и программном обеспечении с открытым исходным кодом, используемых в сетях связи, устройствах конечного пользователя или иных устройствах на базе любого другого вида информационно-коммуникационных технологий (ИКТ), способных использовать программное обеспечение. В CVE содержится только стандартный номер идентификатора с индикатором состояния, краткое описание и ссылки на соответствующие сообщения об уязвимостях и инструкции.

Репозитарий идентификаторов CVE доступен по адресу:
cve.mitre.org/cve/cve.html.

Malware Attribute Enumeration and Characterization (MAEC™)



<https://maecproject.github.io/>

Язык перечня и характеристик атрибутов вредоносного программного обеспечения (МАЕС) включает перечни атрибутов и видов поведения вредоносного программного обеспечения, которые образуют общий словарь.

Эти перечни относятся к разным уровням абстракции: “Наблюдаемые” (Observables) низкого уровня, виды поведения среднего уровня и таксономии высокого уровня.

Рекомендация МСЭ-Т Х.1546, касающаяся использования перечня и характеристик атрибутов вредоносного программного обеспечения (МАЕС), направлена на стандартизацию передачи этой информации по всему спектру средств и услуг обеспечения безопасности, которые могут использоваться для мониторинга и управления защитой от вредоносного программного обеспечения.

МАЕС – это язык, который используется для кодирования подробной информации, относящейся к вредоносному программному обеспечению.

Malware Attribute Enumeration and Characterization (MAEC™)



Анализ угроз, обнаружение вторжения и управление инцидентами – это процессы, которые касаются всех типов киберугроз.

Благодаря единообразному кодированию атрибутов вредоносного программного обеспечения, язык MAEC предоставляет стандартный формат для включения в эти процессы информации, позволяющей принять меры, которая касается вредоносного программного обеспечения.

В настоящее время существует несколько распространенных методов, используемых для обнаружения вредоносного программного обеспечения, которые основаны, главным образом, на физических сигнатаурах и эвристике.

Эти методы эффективны с точки зрения их узкой направленности, хотя им присущи индивидуальные недостатки. *Например, известно, что сигнатуры непригодны для противодействия вирусам "нулевого дня", целевым и полиморфным вирусам, а также другим видам появляющегося вредоносного программного обеспечения.*

Аналогичным образом, эвристическое обнаружение способно в общем обнаруживать определенные типы вредоносного программного обеспечения и при этом пропускать те из них, для которых отсутствуют шаблоны, например руткиты уровня ядра.

Cyber Observable eXpression (CybOX™)

<https://cyboxproject.github.io/>

CybOX has been integrated into Version 2.0 of Structured Threat Information eXpression (STIX™).



СybOX – это стандартизованный язык описания, сбора, определения характеристик и обмена информацией о событиях или свойствах, отражающих состояние, которые наблюдаются в операционном домене.

"Кибернаблюдаемые" имеют отношение ко многим доменам, в том числе оценке и характеристикам угроз (подробные схемы атак), характеристикам вредоносного программного обеспечения, управлению операционными событиями, регистрации событий, осведомленности о ситуации в киберпространстве, реагированию на инциденты, цифровому экспертно-техническому анализу и обмену информацией о киберугрозах.

"Кибернаблюдаемое" – это измеряемое событие или отражающее состояние свойство в кибердомене.

Примеры измеряемых событий включают создание ключа системного реестра, удаление файла и прием запроса HTTP GET;

примеры отражающих состояния свойств включают хэш-функцию MD5 какого-либо файла, значение ключа системного реестра и наличие взаимоисключений.

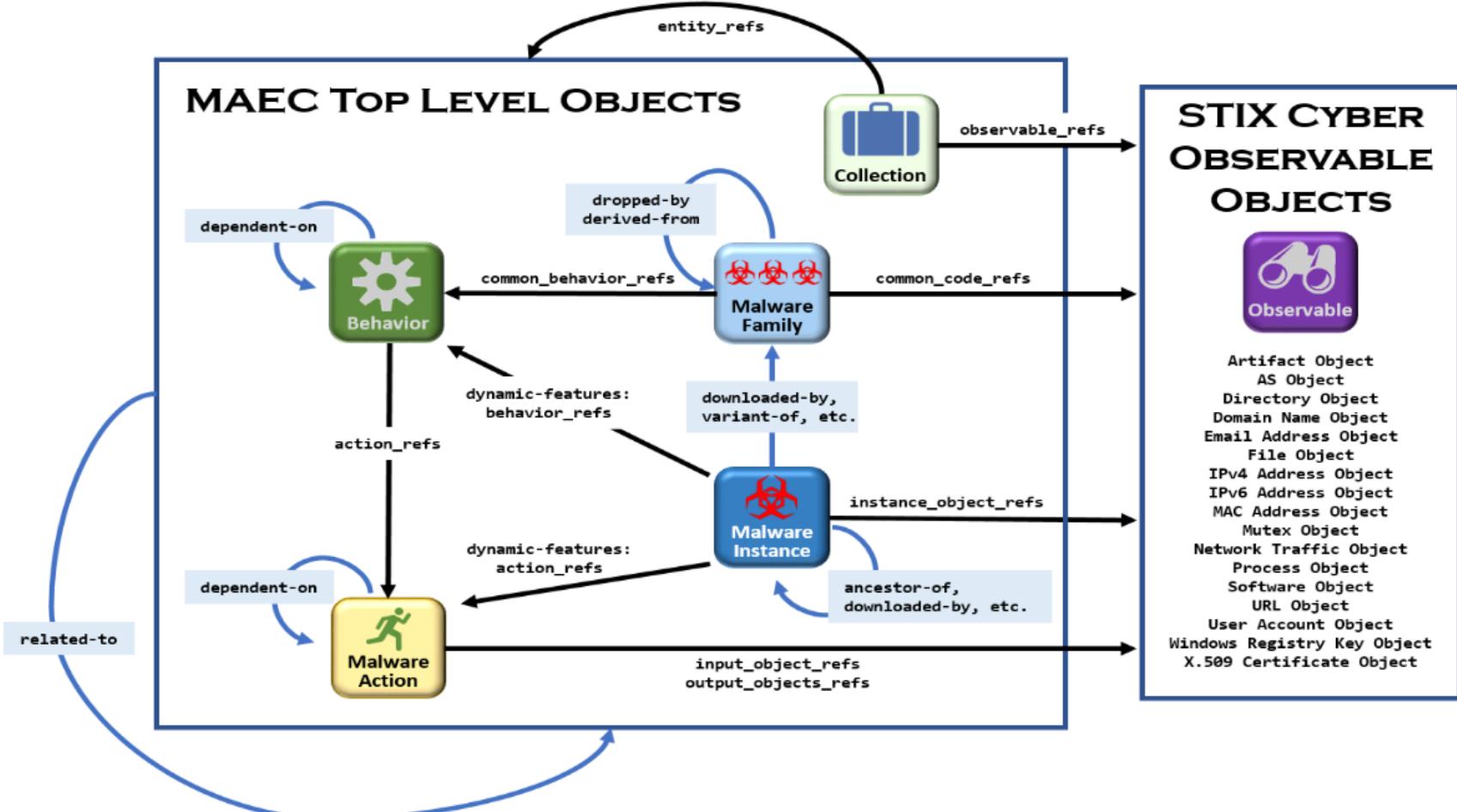
Structured Threat Information eXpression — STIX™

<https://oasis-open.github.io/cti-documentation/stix/intro>



Модель данных MAEC может быть представлена в виде связного графа узлов и ребер, где объекты верхнего уровня MAEC определяют узлы, а отношения MAEC определяют ребра. Связь - это связь между объектами MAEC, которая описывает, как объекты связаны.

Как показано на схеме, MAEC определяет несколько объектов верхнего уровня: поведения, действия вредоносного ПО, семейства вредоносных программ, экземпляры вредоносных программ и коллекции. Отношения между объектами (включая кибер-наблюдаемые объекты с выражением структурированной информации об угрозах (STIX™)) изображаются направленными дугами на диаграмме: встроенные связи (те, которые указаны непосредственно в объекте верхнего уровня в качестве свойства объекта) помечены черным шрифтом (метки соответствуют именам свойств), а прямые отношения помечаются синим фоном (метки соответствуют буквальным значениям для типа отношения).



Модель агрегации данных в кибербезопасности из различных источников NIST SCAP

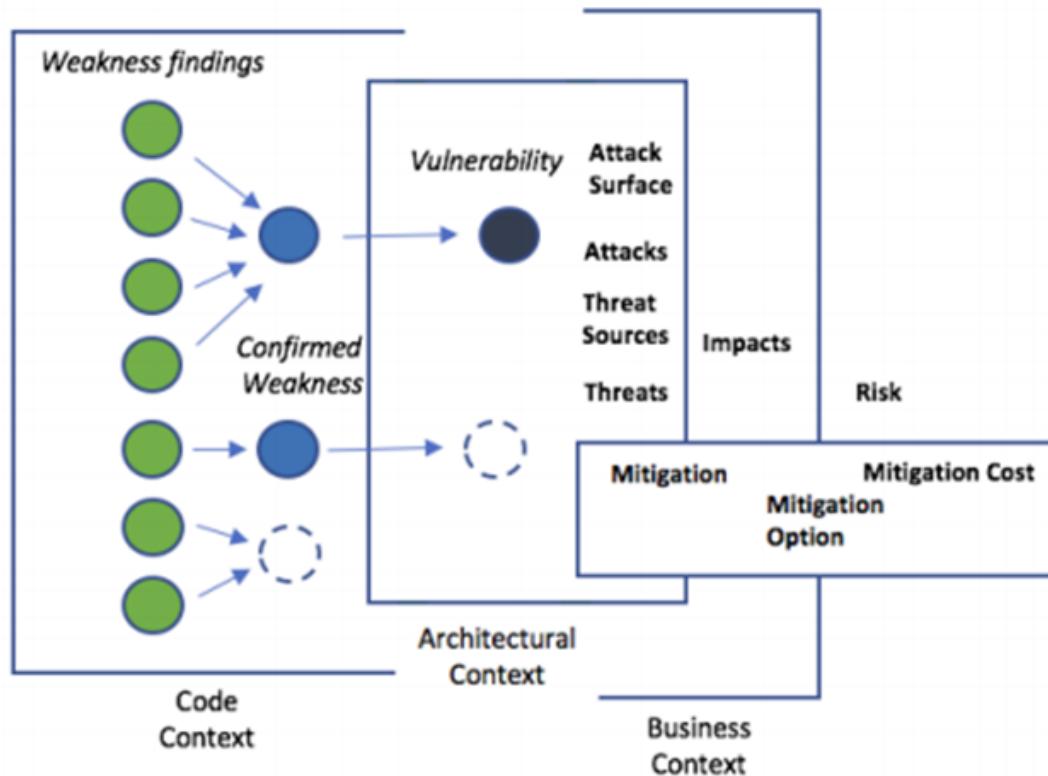
При разработке системы измерения слабых мест (weakness) и уязвимостей (vulnerability) для отдельной исследуемой системы, возникают проблемы агрегации данных из различных источников.

Static Code Analysis (SCA) выполняет анализ контроля и потока данных в коде.

Проблемы:

1. недостаточный контекст для анализа, который приводит к ситуации, когда инструменту SCA неизвестны полный контроль и поток данных, или неизвестны последствия слабых мест.
2. сообщение об уязвимости (vulnerability) - это оппортунистический процесс, когда об уязвимости сообщается в отношении известного коммерческого продукта, она уже подтверждена и последствия хорошо изучены.
3. архитектурные аспекты: какие вычисления вызовут сбои? Насколько они важны? Сколько их? Как злоумышленник может контролировать вычисления и вводить данные?
4. необходимо учитывать важность и расположение актива и имеющиеся контроли безопасности на пути злоумышленника в систему. Например, в метрической системе CWSS группа показателей области атаки – это барьеры, которые должен преодолеть злоумышленник, для того чтобы эксплуатировать слабое место и получить доступ к активу.
5. актив – системный компонент, он может быть реализован несколькими модулями, каждый из которых имеет несколько недостатков.

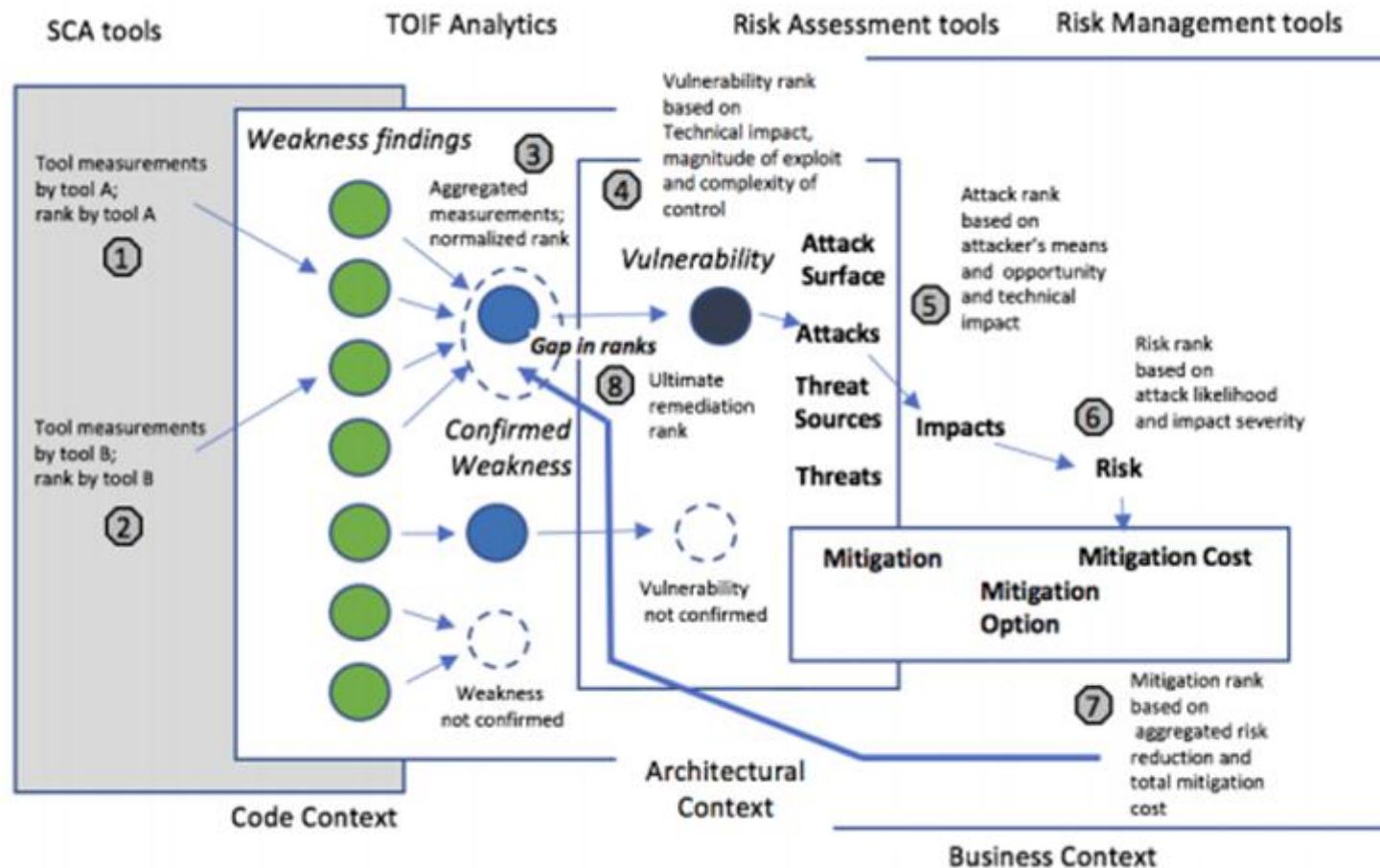
Модель взаимодействия (связи) атрибутов и управления ИБ: Архитектурный контекст



Поток информации идет от сообщения о слабости одного или нескольких инструментов SCA к **“подтвержденной слабости”**, к **уязвимости безопасности**, которая представляет собой уязвимое место, которое можно использовать. Уязвимость связана с успешными атаками на всю развернутую систему.

Оценка состояния безопасности системы включает в себя понимание того, как система может быть атакована (построение шаблона атак), какие характеристики системы делают некоторые атаки успешными (которые по определению являются уязвимостями), какие субъекты угроз способны и мотивированы для запуска атак, а также каковы последствия атак.

Модель взаимодействия (связи) атрибутов и управления ИБ: Архитектурный контекст



На рисунке показано, что в сквозном процессе управления рисками задействовано до 8 различных рангов. Исходный ранг (блок 1,2) может быть сгенерирован инструментом SCA, анализирующим код компонента в программном обеспечении. Когда исходные измерения инструмента агрегируются для каждой подтвержденной слабости, может быть получен нормализованный ранг (блок 3). Ранжирование уязвимостей (блок 4) определяется в первую очередь архитектурными соображениями, включая анализ источников угроз, их средств и возможностей, поверхности атаки, точек входа, зависимостей между возможностями и процессами системы. Ранжирование атак (блок 5), Рейтинг рисков (блок 6), Смягчения последствий (блок 7), Приоритет для исправления (блок 8).

Анализ архитектурных особенностей информационных систем

Анализ архитектурного решения анализируемой информационной системы позволяет использовать описание различных угроз и связанных с ними параметров в области информационной безопасности.

Такое решение должно предоставлять аналитику информацию об:

- **информационные объекты** (например, создание ключа реестра, сетевой трафик на определенные IP-адреса, отправка email с определенного адреса и т.д.);
- **знание целевых платформ**, API, описывающих точки входа и выхода;
- **индикаторы IoC; инциденты**;
- **тактики, методы, процедуры атакуемого** (шаблоны атак САРЕС, вредоносные программы МАЕС, эксплойты и т. д.);
- **объекты эксплуатации** (например, уязвимости, ошибки безопасности или неправильные конфигурации);
- **способы противодействия** (реагирование на инциденты или устранение уязвимостей/ошибок безопасности);
- **группы кибер-атак** (наборы инцидентов, TTP STIX);
- **участники киберугроз** (идентификация, характеристики противника).

Модель безопасности STRIDE-LM

STRIDE-LM	Threat	Property	Definition	Controls
S	Spoofing	Authentication	Impersonating someone or something	Authentication Stores, Strong Authentication mechanisms
T	Tampering	Integrity / Access Controls	Modifying data or code	Crypto Hash, Digital watermark/ isolation and access checks
R	Repudiation	Non-repudiation	Claiming to have not performed a specific action	Logging infrastructure, full-packet-capture
I	Information Disclosure	Confidentiality	Exposing information or data to unauthorized individuals or roles	Encryption or Isolation
D	Denial of Service	Availability	Deny or degrade service	Redundancy, failover, QoS, Bandwidth throttle
E	Elevation of Privilege	Authorization / Least Privilege	Gain capabilities without proper authorization	RBAC, DACL, MAC; Sudo, UAC, Privileged account protections
LM	Lateral Movement	Segmentation / Least Privilege	Expand influence post-compromise; often dependent on Elevation of Privilege	Credential Hardening; Segmentation and Boundary enforcement; Host-based firewalls

Модель категоризации **STRIDE-LM** включает определения, соответствующее свойство безопасности и элементы управления, связанные с типом угрозы по умолчанию.

Модель угроз идентифицирует основные типы угроз, которые затем напрямую ссылаются на соответствующее свойство и тип элемента управления.

Например, угроза **Information Disclosure** (STRIDE-LM) имеет соответствующее свойство безопасности Confidentiality и типы управления Encryption или Isolation. Эта прямая ссылка от категоризации угроз к контролю является основополагающей концепцией подхода, основанного на угрозах.

Модель безопасности STRIDE-LM

Spoofing (Подмена) – атаки заключаются в использовании учетных данных другого пользователя без его ведома, а типичные угрозы нацелены на слабые механизмы аутентификации.

Tampering (Вмешательство) – если злоумышленник может вмешаться в систему, это может иметь некоторые последствия для её использования, например, если злоумышленник может добавить или удалить некоторые функциональные элементы, или для целей системы, например, если важные данные будут уничтожены или изменены.

Repudiation (Отказ) – злоумышленники часто хотят скрыть свою вредоносную активность, чтобы избежать обнаружения и блокировки, поэтому они могут попытаться отказаться от выполненных действий, например, удалив их из журналов или подделав учетные данные другого пользователя.

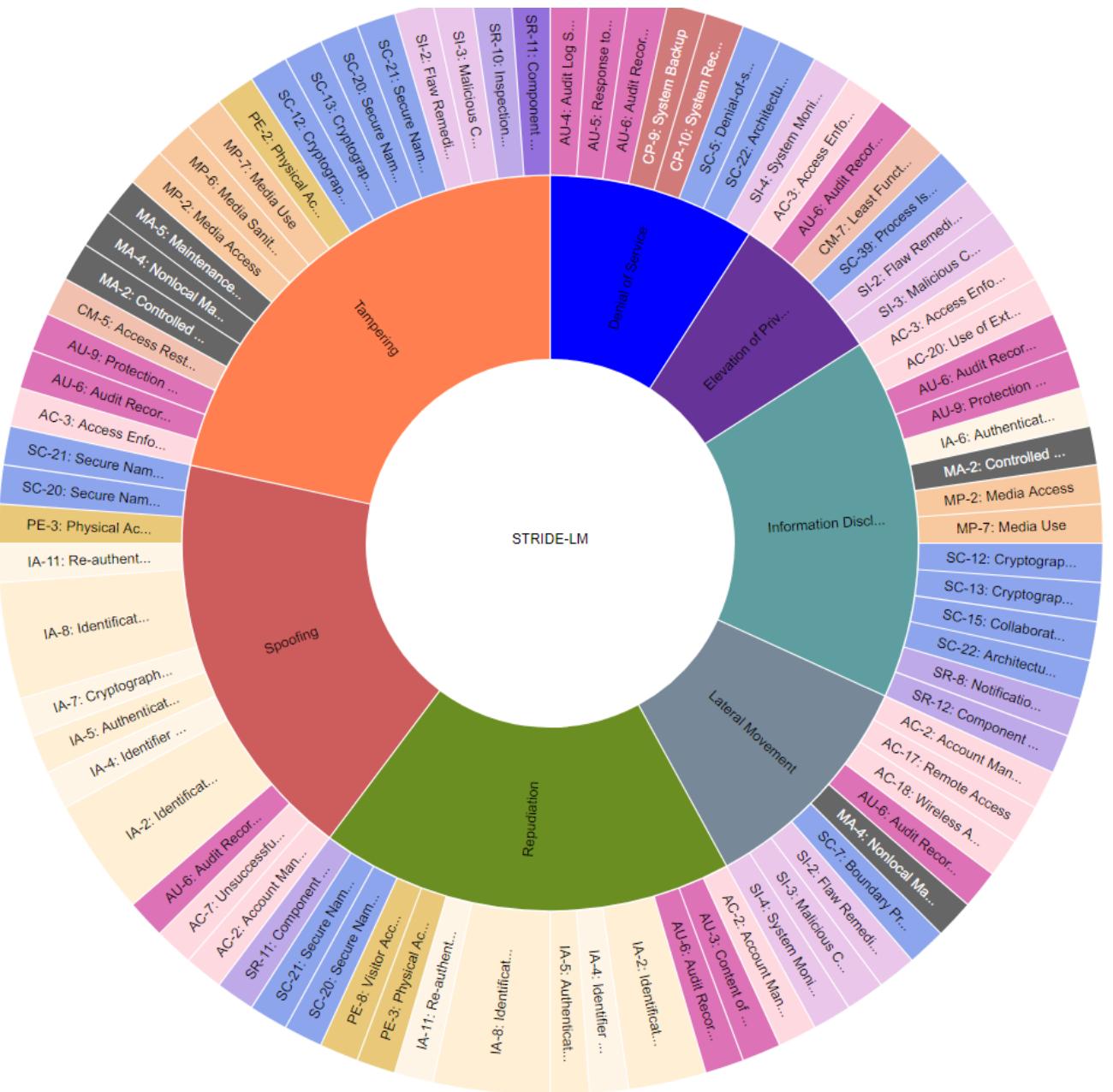
Information disclosure (Раскрытие информации) – многие системы содержат конфиденциальную информацию, и злоумышленники часто стремятся завладеть ею.

Denial of service (Отказ в обслуживании) – в некоторых случаях злоумышленники будут заинтересованы в том, чтобы помешать обычным пользователям получить доступ к системе, например, для шантажа и вымогательства денег у владельца системы.

Escalation of privilege (Повышение привилегий) – злоумышленник может попытаться получить дополнительные привилегии, например, подделав пользователя с более высокими привилегиями или изменив систему, чтобы изменить свои собственные привилегии

Lateral Movement (Горизонтальное изменение привилегий, боковое движение) - расширение контроля над целевой сетью за пределы начальной точки компрометации.

Хороший сайт: <https://csf.tools/reference/stride-lm/>



Визуализация параметров STRIDE-LM и контролей безопасности NIST SP 800-53 Security Controls

Structured Threat Information eXpression — STIX™

A Structured Language for Cyber Threat Intelligence Information.

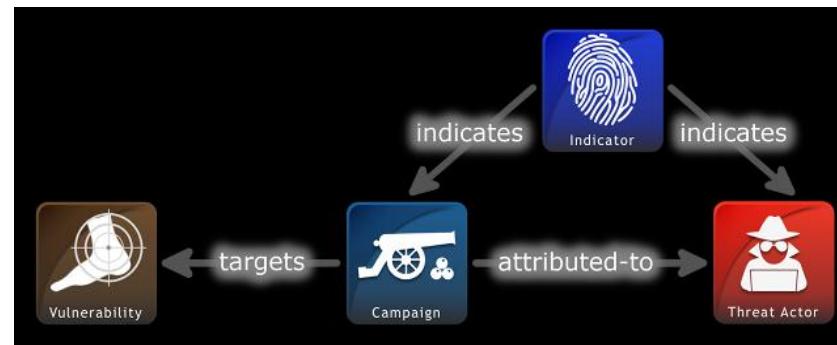
Структурированный язык для описания угроз ИБ



Trusted Automated eXchange of Indicator Information — TAXII™.

Enabling Cyber Threat Information Exchange.

*Доверенный формат обмена
индикаторами угроз.*



К.т.н., доцент ИКТИБ ЮФУ
Князева Маргарита Владимировна

STIX(Structured Threat Information eXpression)

STIX (Structured Threat Information eXpression) - стандарт, используемый для предоставления унифицированной информации о киберугрозах (CTI).

CIT (Cyber threat intelligence) - is information about threats and threat actors that helps mitigate harmful events in cyberspace. Cyber threat intelligence sources include open source intelligence, social media intelligence, human Intelligence, technical intelligence or intelligence from the deep and dark web.

Позволяет совместно использовать описание различных угроз и связанных с ними параметров в различных областях.

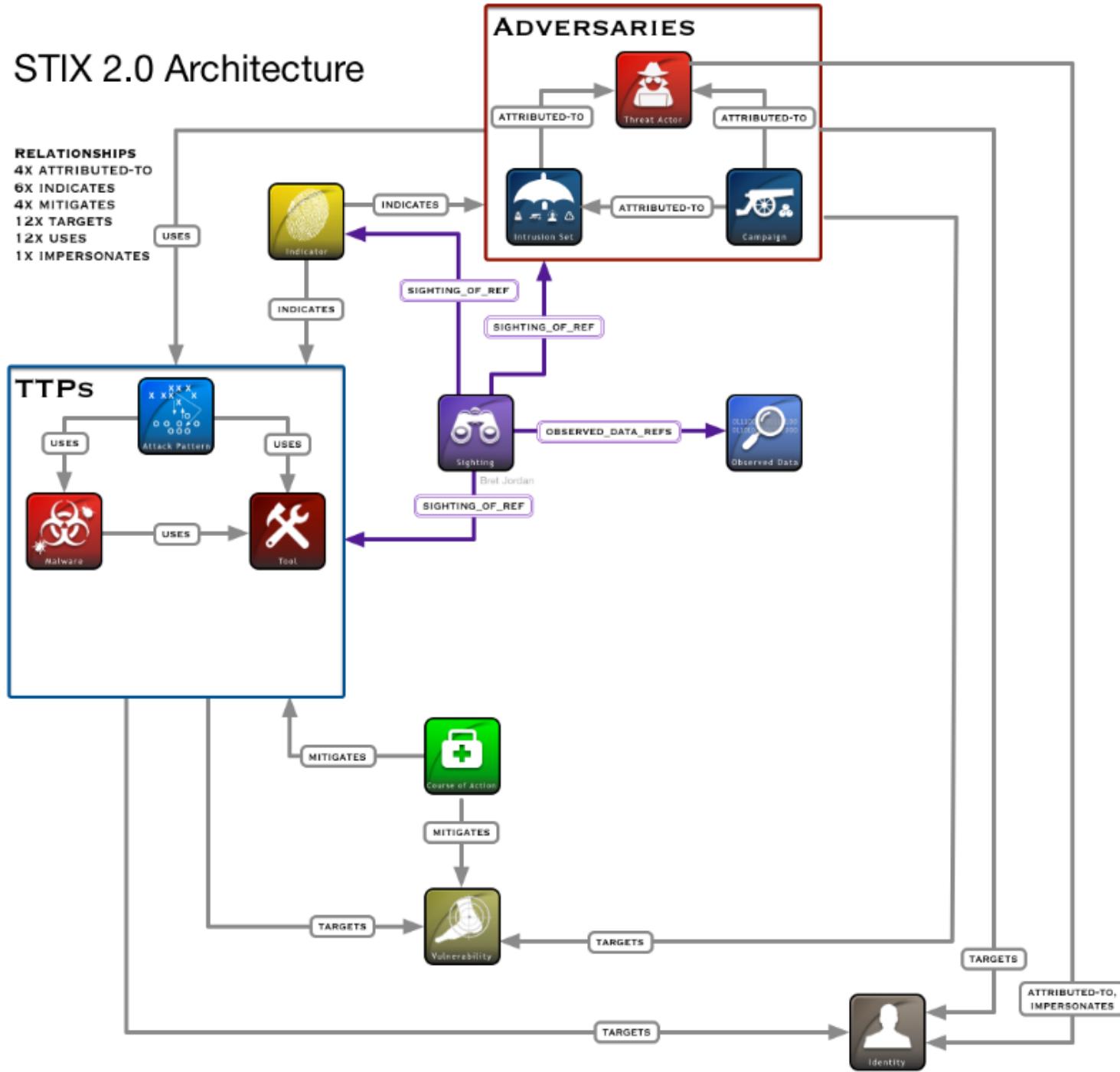
STIX предоставляет унифицированную информацию об инцидентах, включая:

- ✓ информационные объекты (например, создание ключа реестра, сетевой трафик на определенные IP-адреса, отправка email с определенного адреса и т.д.);
- ✓ индикаторы; инциденты;
- ✓ тактики, методы, процедуры атакуемого (шаблоны атак, вредоносные программы, эксплойты и т. д.);
- ✓ объекты эксплуатации (например, уязвимости, ошибки безопасности или неправильные конфигурации);
- ✓ способы противодействия (реагирование на инциденты или устранение уязвимостей/ошибок безопасности);
- ✓ группы кибер-атак (наборы инцидентов, TTP);
- ✓ участники киберугроз (идентификация, характеристики противника).

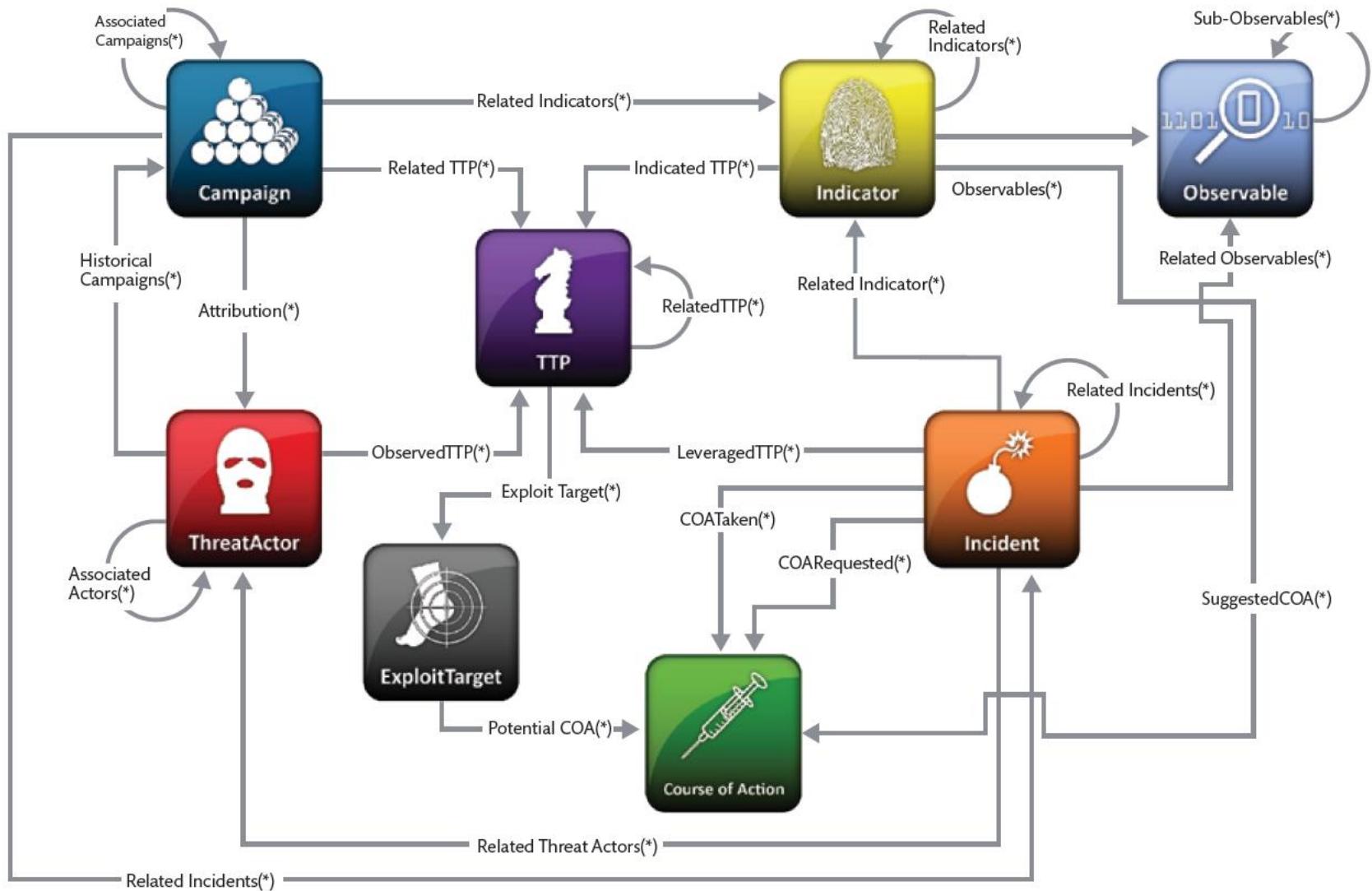
- *MITRE (Mitre Corporation) — крупная американская некоммерческая организация, специализирующаяся в области системной инженерии и ведущая разработки и исследования в интересах органов государственной власти США, таких как Министерство обороны США, Федеральное управление гражданской авиации США и др.. Базируется в городах Бедфорд (Массачусетс) и Маклин (Вирджиния).*
- <https://stixproject.github.io/>



STIX 2.0 Architecture



Архитектура STIX - Objects





Attack Pattern (Шаблон Атаки)

A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.



Campaign (Кампания)

A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.



Course of Action (Курс действий)

An action taken to either prevent an attack or respond to an attack.



Identity (Идентификация)

Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.



Indicator (Индикатор)

Contains a pattern that can be used to detect suspicious or malicious cyber activity.



Intrusion Set (Множество вторжений)

A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.



Malware (Вирусы)

A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.



Observed Data (Анализируемая инф.)

Conveys information observed on a system or network (e.g., an IP address).



Report (Отчеты)

Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.



Threat Actor (Актор, злоумышленник)

Individuals, groups, or organizations believed to be operating with malicious intent.



Tool (Инструменты)

Legitimate software that can be used by threat actors to perform attacks.



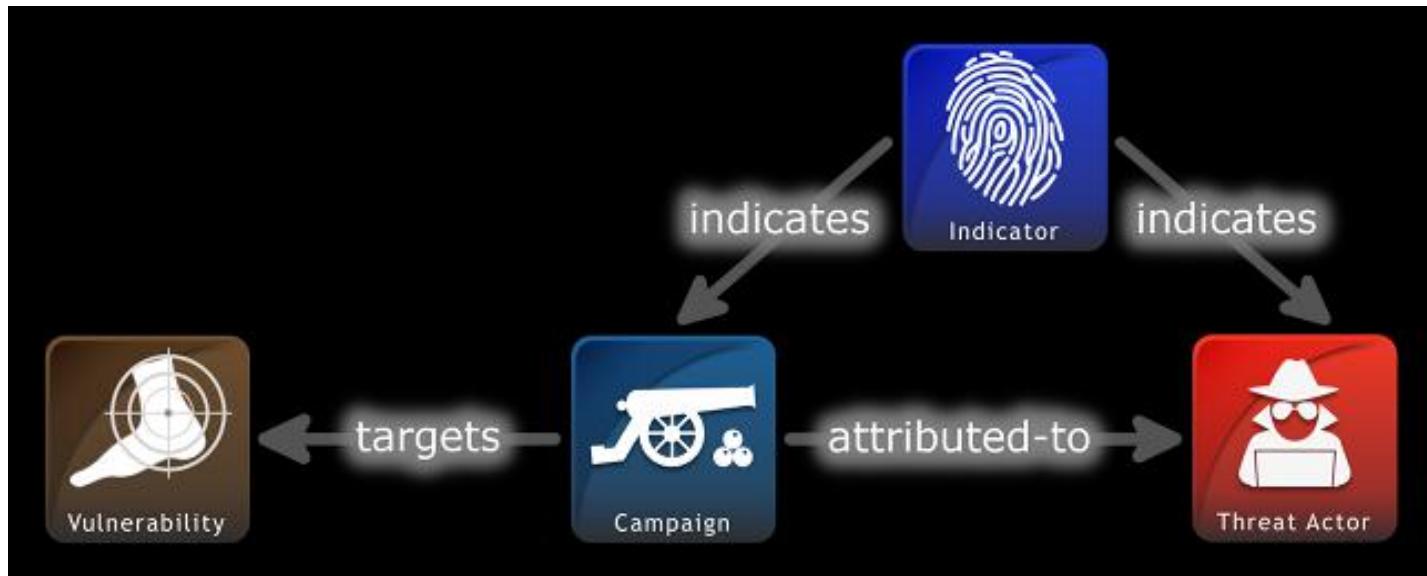
Vulnerability (Уязвимости)

A mistake in software that can be directly used by a hacker to gain access to a system or network.

STIX(Structured Threat Information eXpression)

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).

Pecypc: <https://oasis-open.github.io/cti-documentation/stix/intro#stix-21-defines-18-stix-domain-objects-sdos>



STIX (Structured Threat Information eXpression)

CybOX (Cyber Observable eXpression) — стандарт, обеспечивающий общую структуру для описания и представления индикаторов наблюдаемых событий безопасности. На текущий момент уже представлено свыше 70 различных наблюдаемых объектов: файл, сетевое соединение, HTTP-сессия, сетевой трафик, сертификат X.509 и т.п.

TLP (Traffic Light Protocol) — протокол, позволяющий «раскрасить» информацию в четыре цвета, влияющих на то, кому можно передавать полученную информацию об угрозах.

IODEF (Incident Object Description and Exchange Format) (RFC 5070) — стандарт, содержит в формате XML свыше 30 классов и подклассов инцидентов, включая информацию о контактах, нанесенном финансовом ущербе, времени, пострадавшие операционные системы и приложения и т.д. IODEF — стандарт достаточно проработанный и уже немало где используется. IODEF- SCI (IODEF for Structured Cyber Security Information) – расширение для IODEF, позволяющее добавлять к IODEF дополнительные данные: шаблоны атак, информацию о платформах, уязвимостях, инструкциях по нейтрализации, уровень опасности и т.п.

OpenIOC (Indicator of Compromise) — открытый стандарт описания индикаторов компрометации. Построен на базе XML и содержит свыше 500 различных индикаторов, преимущественно узловых (хостовых) — файл, драйвер, диск, процесс, реестр, система, хэш и т. п.

MISP — открытый формат для структурированного описания индикаторов, информации об угрозах, акторах, финансовом фроде, в основе лежит JSON.

VERIS (Vocabulary for Event Recording and Incident Sharing) — стандарт для описания угроз и инцидентов. Схема VERIS состоит из пяти частей:

- ✓ Incident Tracking;
- ✓ Victim Demographics;
- ✓ Incident Description;
- ✓ Discovery & Response;
- ✓ Impact Assessment.

TAXII (Trusted Automated Exchange of Intelligence Information) — стандарт, используемый для унификации способов обмена информацией о киберугрозах (CTI) по протоколу HTTPS, описанных с помощью STIX.

VEDEF (Vulnerability and Exploit Description and Exchange Format) — стандарт для обмена информацией об уязвимостях и эксплойтах.

Indicators of Attack (IoA) vs. Indicators of Compromise (IoC)

! Характерные признаки компрометации - это имеющие определенное состояние свойства и измеряемые события безопасности, связанные с работой компьютеров и сетей.

!! Индикаторы компрометации IoC (Computer Forensics) - это конструкции, доказательства после инцидента, используемые для подачи характерных признаков компрометации в совокупности с контекстной информацией с целью представления артефактов и/или заслуживающего внимания поведения в контексте кибербезопасности, например, хэш MD5, С&С-домен, прописанный в коде IP-адрес, ключ реестра, имя файла и др. Они постоянно изменяются.

!!! Индикаторы атаки IoA – это набор конструкций, состоящий из неизвестных атрибутов, индикаторов компрометации IoC, контентной и контекстной информации, анализируемой в режиме реального времени, динамически.

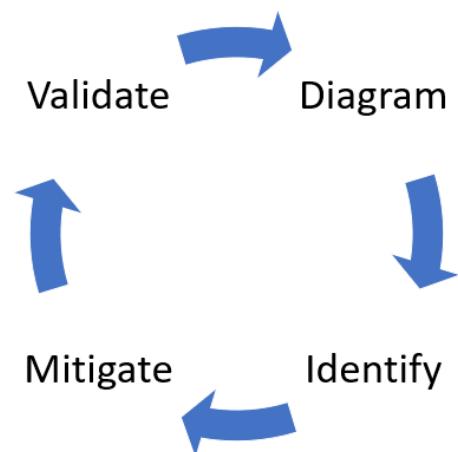


МОДЕЛИРОВАНИЕ РИСКОВ ИБ: DREAD, STRIDE, 5A

COMMON VULNERABILITY SCORING SYSTEM - CVSS 3.0

Руководство по оценке рисков безопасности

Доцент ИКТИБ, к.т.н., Князева М.В.



Управление рисками ИБ

Управление рисками информационной безопасности по своей сути является ядром системы менеджмента информационной безопасности (СМИБ).

Составляющими процесса управления рисками являются процедуры своевременного выявления рисков (risk identification), их оценка (risk assessment) и последующая обработка (risk treatment).

Методология оценки рисков информационной безопасности предусматривает такие шаги, как:

- выявление уязвимостей (организационных и технических);
- выявление угроз, направленных на рассматриваемые активы;
- определение последствий от реализации угроз;
- выявление существующих контролей (контрмер);
- определение вероятности реализации угроз.

Методики оценки уязвимостей

Для оценки рисков уязвимостей технических информационных систем традиционно применяются различные подходы:

- системы оценки угроз, как например, системы, используемые Министерством безопасности США и центром Sans Internet Storm Center. Эти службы предоставляют систему предупреждений об опасностях критически важным IT-сетям в США и в мире соответственно.
- базы данных уязвимостей, как National Vulnerability Database (NVD), Open Source Vulnerability Database (OSVDB) или Bugtraq. Эти базы данных представляют собой каталог известных уязвимостей с подробной дополнительной информацией.
- системы идентификации уязвимостей, как, например стандарт Common Vulnerabilities and Exposures (CVE) или словарь уязвимостей Common Weakness Enumeration (CWE). Эти системы используются для того, чтобы однозначно идентифицировать и классифицировать уязвимости в соответствии с тем, где они обнаружены – в коде, при разработке или в архитектуре.

Системы оценки уязвимостей

Для оценки рисков уязвимостей технических информационных систем традиционно применяются две методики:

1. DREAD - аббревиатура факторов, которые учитывает эта шкала:

- **damage potential**, — оценка ущерба от реализации угроз через эксплуатацию уязвимости;
- **reproducibility**, — воспроизводимость способа эксплуатации уязвимости;
- **exploitability**, — легкость эксплуатации уязвимости;
- **affected users**, — оценка аудитории пользователей, затрагиваемых при реализации угроз через эксплуатацию уязвимости;
- **discoverability**, — обнаруживаемость уязвимости.

Для каждой из выявленных уязвимостей, перечисленных факторам дается оценка от 0 до 10 и рассчитывается суммарное значение риска по формуле:

$$Risk_DREAD = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5$$

Методики оценки уязвимостей компонент

МСЭ-Т СЕКТОР СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ МСЭ
СЕРИЯ Х: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАЙМОСВЯЗЬ ОТКРЫТЫХ
СИСТЕМ И БЕЗОПАСНОСТЬ, Обмен информацией, касающейся
кибербезопасности – Обмен информацией
об уязвимости/состоянии

X.1521(03/2016) Система оценки общеизвестных уязвимостей 3.0 (4/0)

CVSS (Common Vulnerability Score System)

В описаниях уязвимостей векторы типа AV:N/AC:L/Au:N/C:N/I:N/A:C

Спецификация шкалы: <https://www.first.org/cvss>

Калькулятор: <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>



CVSS v3.0 Calculator [?]

Medium 4.3

Attack Vector [?]	Network	Adjacent	Local	Physical	Scope [?]	Unchanged	Changed
Attack Complexity [?]	Low	High	Confidentiality [?]	None	Low	High	
Privileges Required [?]	None	Low	Integrity [?]	None	Low	High	
User Interaction [?]	None	Required	Availability [?]	None	Low	High	

Методики оценки уязвимостей компонент



About FIRST ▾ Membership ▾ Initiatives ▾ Standards & Publications ▾ Events ▾ Education ▾ Blog



Table of Contents

- Common Vulnerability Scoring System version 4.0: Specification Document**
- Introduction**
 - Metrics
 - Assessment
 - Nomenclature
- Base Metrics**
 - Exploitability Metrics
 - Impact Metrics
- Threat Metrics**
 - Exploit Maturity (E)
- Environmental Metrics**
 - Confidentiality, Integrity, and Availability Requirements (CR, IR, AR)
 - Modified Base Metrics
- Supplemental Metrics**
 - Safety (S)
 - Automatability (AU)
 - Provider Urgency (U)
 - Recovery (R)
 - Value Density (V)
 - Vulnerability Response Effort (RE)
- Qualitative Severity Rating Scale**
- Vector String**
- CVSS v4.0 Scoring**
 - New Scoring System Development
 - CVSS v4.0 Scoring using MacroVectors and Interpolation
 - Scores of all MacroVectors
- Appendix A - Acknowledgments**
- Appendix B - On-Line Resources**



Common Vulnerability Scoring System version 4.0: Specification Document

Also available in PDF format [↗](#).

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of four metric groups: Base, Threat, Environmental, and Supplemental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Threat group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. Base metric values are combined with default values that assume the highest severity for Threat and Environmental metrics to produce a score ranging from 0 to 10. To further refine a resulting severity score, Threat and Environmental metrics can then be amended based on applicable threat intelligence and environmental considerations. Supplemental metrics do not modify the final score, and are used as additional insight into the characteristics of a vulnerability. A CVSS vector string consists of a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 4.0.

The most current CVSS resources can be found at <https://www.first.org/cvss/>

CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. FIRST reserves the right to update CVSS and this document periodically at its sole discretion. While FIRST owns all rights and interest in CVSS, it licenses it to the public freely for use, subject to the conditions below. Membership in FIRST is not required to use or implement CVSS. FIRST does, however, require that any individual or entity using CVSS give proper attribution, where applicable, that CVSS is owned by FIRST and used by permission. Further, FIRST requires as a condition of use that any individual or entity which publishes CVSS data conforms to the guidelines described in this document and provides both the score and the vector string so others can understand how the score was derived.

Introduction

The Common Vulnerability Scoring System (CVSS) captures the principal technical characteristics of software, hardware and firmware vulnerabilities. Its outputs include numerical scores indicating the severity of a vulnerability relative to other vulnerabilities.

CVSS is composed of four metric groups: Base, Threat, Environmental, and Supplemental. The Base Score reflects the severity of a vulnerability according to its intrinsic characteristics which are constant over time and assumes the reasonable worst-case impact across different deployed environments. The Threat Metrics adjust the severity of a vulnerability based on factors, such as the availability of proof-of-concept code or active exploitation. The Environmental Metrics further refine the resulting severity score to a specific computing environment. They consider factors such as the presence of mitigations in that environment and the criticality attributes of the vulnerable system. Finally,

<https://www.first.org/cvss/v4.0/specification-document>

Пользователи CVSS

CVSS используется многими организациями, и каждая получает оценку своим способом.

- Поставщики бюллетеней с описанием уязвимости
- Разработчики программных приложений
- Организации-пользователи
- Сканирование уязвимостей и управление уязвимостями
- Управление (рисками) безопасности
- Исследователи



Методика оценки рисков

Общая система оценки уязвимостей [*Common Vulnerability Scoring System, CVSS*], версия 2.0 (3.0) – открытая схема для обмена и оценки уязвимостей ИТ. В этой системе используются группы метрик, а также дается описание базовых метрик [*base metrics*], вектора уязвимости [*vector*] и оценок уязвимости.

3 Группы метрик CVSS 2.0:

- I. *Базовые метрики*: используются для описания основополагающих сведений об уязвимости — возможности эксплуатации уязвимости и воздействии уязвимости на систему, не изменяются со временем и не зависят от среды.
- II. *Временные метрики [temporal]*: при оценке метрики учитывается время, например, опасность уязвимости [*severity of the vulnerability*] снижается с выходом официального обновления безопасности [*official patch*].
- III. *Контекстные метрики [environmental]*: вопросы контекста, среды принимаются во внимание при оценке опасности уязвимости. Например, чем больше систем подвержены [*affected*] уязвимости, тем выше ее опасность.



Методика оценки рисков

Базовые метрики



Существуют метрики возможности эксплуатации [*exploitability*] и воздействия [*impact*]:

I. Возможность эксплуатации

a) **Вектор доступа [access vector, AV]** описывает возможный способ эксплуатации уязвимости:

- локальный [*local*, *L*]— уязвимость эксплуатируется только локально;
- локально-сетевой [*adjacent network*, *A*]— уязвимость может эксплуатироваться только из смежных сетей;
- сетевой [*network*, *N*]—уязвимость может эксплуатироваться удаленно.

Чем дальше может находиться источник атаки, тем опаснее уязвимость.

б) **Сложность доступа [access complexity, AC]** описывает уровень сложности атаки:

- Высокий уровень [*high*, *H*]— для эксплуатации уязвимости требуется выполнить определенную последовательность действий;
- Средний уровень [*medium*, *M*]— уязвимость нельзя отнести ни к сложной, ни к легкоэксплуатируемой;
- Низкий уровень [*low*, *L*]—уязвимость эксплуатируется просто.

Чем ниже оценка сложности доступа, тем опаснее уязвимость.

в) **Метрика «аутентификация» [authentication, Au]** описывает способ аутентификации для эксплуатации уязвимости:

- Многократная [*multiple*, *M*]— атакующий должен пройти аутентификацию два и более раз;
- Однократная [*single*, *S*]— атакующий должен пройти аутентификацию один раз;
- Нулевая [*none*, *N*]—аутентификация не требуется.

Чем меньше раз требуется проходить аутентификацию, тем опаснее уязвимость.



Методика оценки рисков



Значение метрики <i>Access Vector (AV)</i>	Описание
Локальный (L)	Для эксплуатации уязвимости злоумышленник должен иметь локальный доступ, т.е. физический доступ к системе или локальную учетную запись. Примерами таких уязвимостей могут служить атаки на внешние устройства, например, атаки Firewire/USB DMA, и локальное повышение привилегий (например, Sudo).
Соседняя сеть (A)	Для эксплуатации уязвимости злоумышленник должен иметь доступ к соседней сети, т.е. такой сети, которая имеет общую среду передачи с сетью, где находится уязвимое ПО. Например, локальные IP subnet, Bluetooth, IEEE 802.11 и локальные Ethernet-сегменты.
Сетевой (N)	Для эксплуатации уязвимости злоумышленник должен обладать доступом к уязвимому ПО, причем этот доступ ограничен только величиной сетевого стека. Локального доступа или доступа из соседней сети не требуется. Такие уязвимости часто называют эксплуатируемыми удаленно. Примером такой сетевой атаки служит переполнение буфера RPC.

Методика оценки рисков



Значение метрики Access Complexity (AC)	Описание
Высокое (H)	<p><u>Для эксплуатации уязвимости нужны особые условия.</u> Например:</p> <ul style="list-style-type: none"> • В большинстве конфигураций злоумышленник должен иметь повышенные привилегии или эксплуатировать уязвимости одновременно и в других системах (например, захват DNS). • Атаки, основанные на методах социальной инженерии, могут быть легко обнаружены хорошо осведомленными людьми. Например, жертва может выполнить некоторые нетипичные действия. • Уязвимая конфигурация на практике встречается очень редко. • Окно при условиях “race condition” очень узкое. <p>*Состояние гонки (англ. race condition) — ошибка проектирования многопоточной системы или приложения, при которой работа системы или приложения зависит от того, в каком порядке выполняются части кода.</p>

Методика оценки рисков



Значение метрики Access Complexity (AC)	Описание
Среднее (M)	<p><u>Для эксплуатации уязвимости нужны до некоторой степени особые условия.</u> Например:</p> <ul style="list-style-type: none"> • Злоумышленники ограничены группой систем или пользователей, которые имеют некоторый уровень авторизации, и, возможно, являются не доверенными. • Для успешной эксплуатации некоторую информацию необходимо собрать заранее. • Уязвимая конфигурация не является стандартной и обычно не используется (например, уязвимость существует, когда сервер проводит аутентификацию учетной записи пользователя по специальной схеме, но не существует при использовании другой схемы). • Злоумышленнику нужно использовать методы социальной инженерии, чтобы получить некоторое количество информации для обмана осмотрительных пользователей (например, атаки фишинга, которые изменяют статусную строку web-браузера, чтобы показать некорректную ссылку, которая является знакомой и доверенной, до того, как отправить IM-экспloit).
Низкое (L)	

Методика оценки рисков



Значение метрики Access Complexity (AC)	Описание
Низкое (L)	<p><u>Для эксплуатации уязвимости не требуются специальные условия и особые обстоятельства. Например:</u></p> <ul style="list-style-type: none">• Доступ к уязвимому продукту имеют большое количество систем и пользователей, причем доступ может быть анонимный или не доверенный (например, соединенный с Интернетом Web или почтовый сервер).• Уязвимая конфигурация является стандартной или повсеместно используемой/• Атаку можно провести вручную или обладая небольшим количеством навыков. Требуется немного дополнительной информации.• Условия “race condition” легко использовать.

Методика оценки рисков



Базовые метрики

Существуют метрики возможности эксплуатации [*exploitability*] и воздействия [*impact*]:

II. Воздействие

а) Метрика «воздействие на конфиденциальность» [*confidentiality, C*] описывает воздействие уязвимости на конфиденциальность данных системы:

- нулевое [*none, N*]-воздействие отсутствует;
- частичное [*partial, P*]-можно считать часть данных;
- полное [*complete, C*]-можно считать любые данные.

Чем сильнее воздействие на конфиденциальность данных в системе, тем опаснее уязвимость.

б) Метрика «воздействие на целостность» [*integrity, I*] описывает воздействие уязвимости на целостность данных системы:

- нулевое [*none, N*]-воздействие отсутствует;
- частичное [*partial, P*]-можно изменить часть данных;
- полное [*complete, C*]-можно изменить любые данные.

Чем сильнее воздействие на целостность данных в системе, тем опаснее уязвимость.

в) Метрика «воздействие на доступность» [*availability, A*] описывает воздействие уязвимости на доступность системы:

- нулевое [*none, N*]-воздействие отсутствует;
- частичное [*partial, P*]- уязвимость может вызвать в системе временные отказы в обслуживании или снижение производительности;
- полное [*complete, C*]- уязвимость может вызвать полный отказ системы в обслуживании.

Чем сильнее воздействие на доступность системы, тем опаснее уязвимость.

Обратите внимание на сокращенные названия метрик и их значения в скобках. Эти сокращения используются в описании базового вектора уязвимости (см. ниже).



Методика оценки рисков



Временные метрики

NB! Угроза, которую несет уязвимость, может изменяться со временем.

Факторы которые изменяются со временем и учитываются в CVSS:

а) Метрика Exploitability (E) - Возможность использования

Эта метрика отображает наличие или отсутствие кода или техники эксплуатации. Если легкий в использовании код эксплуатации является общедоступным, то число потенциальных злоумышленников резко возрастает, что увеличивает серьезность уязвимости.

Значение показателя	Описание
Непроверенная (Unproven, U)	Код эксплойта не доступен или эксплуатация возможна лишь теоретически.
правильность концепции (Proof-of-Concept, PoC)	Доступен код эксплойта, доказывающий правильность концепции, или существует демонстрация атаки, которая не применима в большинстве систем. Код или метод действуют не во всех ситуациях, и для их использования может потребоваться существенное изменение, внесенное квалифицированным злоумышленником.
Функциональная (Functional, F)	Функциональный код эксплойта доступен и применим в большинстве ситуаций, где существует уязвимость.
Высокая (High, H)	Уязвимость можно эксплуатировать с помощью функционального мобильного автономного кода, или эксплойт не нужен (запуск вручную) и детали широко известны. Код эксплуатации работает в любой ситуации или его активная доставка осуществляется мобильным автономным агентом (например, червем или вирусом).
Не определено (Not Defined, ND)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле данный показатель будет пропущен.

Методика оценки рисков



Временные метрики

Факторы которые изменяются со временем и учитываются в CVSS:

б) Remediation Level (RL) - Уровень исправления

Типичная уязвимость обычно не имеет исправления, когда информация о ней публикуется впервые. Текущие исправления и дополнительные действия предлагаются для временного исправления уязвимости до того момента, когда будет выпущено официальное исправление или обновление.

Значение показателя	Описание
Официальное исправление (Official Fix, OF)	Доступно готовое решение от разработчика, который либо выпустил официальную корректировку, либо предоставил обновление.
Временное исправление (Temporary Fix, TF)	Доступно официальное временное исправление. Например, разработчик выпустил временный модуль оперативной коррекции, средство или опубликовал обходной прием.
Обходной прием (Workaround, W)	Доступно неофициальное решение, которое предоставлено третьей стороной. В некоторых случаях пользователи затронутой технологии создают собственную корректировку или принимают меры для нахождения обходного приема или каким-либо другим способом уменьшают влияние уязвимости.
Недоступно (Unavailable, U)	Решение либо недоступно, либо его невозможно применить.
Не определено (Not Defined, ND)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле данный показатель будет пропущен.

Методика оценки рисков



Временные метрики

Факторы которые изменяются со временем и учитываются в CVSS:

в) Report Confidence (RC) - Степень достоверности отчета

Эта метрика отображает степень конфиденциальности информации о существовании уязвимости и достоверность известных технических деталей. Иногда публикуется только информации о существовании уязвимости, а детали не указываются. Позже уязвимость может быть дополнена информацией о технологии эксплуатации от автора или от производителя. Риск от наличия уязвимости выше, если ее существование достоверно известно.

Значение показателя	Описание
Не подтверждена (Unconfirmed, UC)	Существует единственный неподтвержденный источник или несколько противоречивых сообщений. Достоверность степени валидации этих сообщений мала. Одним из примером является слух, появившийся в хакерских кругах.
Не подкреплена доказательствами (Uncorroborated, UR)	Существует множество неофициальных источников, в том числе, возможно, независимых компаний в области безопасности или исследовательских организаций. На этом этапе могут существовать противоречивые технические детали или некоторая иная затянувшаяся неопределенность.
Подтверждена (Confirmed, C)	Уязвимость признана разработчиком или автором затронутой технологии. Это значение также может быть присвоено уязвимости, если ее существование подтверждено каким-то внешним событием, например, публикацией функционального кода эксплойта или кода эксплойта, доказывающего правильность концепции, либо масштабной эксплуатацией.
Не определено (Not Defined, ND)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле данный показатель будет пропущен.

Методика оценки рисков



Контекстные метрики

NB! Группа контекстных метрик CVSS отражает характеристики уязвимости, которые связаны со средой пользователя.

Факторы которые изменяются со временем и учитываются в CVSS:

а) Collateral Damage Potential (CDP) - Вероятность нанесения косвенного ущерба

Эта метрика отображает потенциальную возможность повреждения или утраты собственности или оборудования, а также может оценивать экономические потери, связанные с производительностью или доходом: (None, N), (Low, L), (Low-medium, LM), (Medium-high, MH), (High, H), (Not defined, ND).

б) Target Distribution (TD) - Плотность целей

Эта метрика отображает процент уязвимых систем от всех имеющихся систем. Она используется как особый индикатор среды, чтобы приблизительно определить процент систем, на которые может влиять данная уязвимость.

в) Security Requirements (CR, IR, AR) - Требования к безопасности

Эти метрики позволяют аналитику определить CVSS-оценку в зависимости от важности уязвимого устройства или программного обеспечения для организации, измеренной в терминах конфиденциальности, целостности и доступности. Это означает, что если уязвимость обнаружена в программном или аппаратном обеспечении, которое отвечает за бизнес-функцию, для которой наиболее важна доступность, аналитик может присвоить большее значение доступности, относительно конфиденциальности и целостности.

*Базовая формула CVSS 2.0

Базовая формула является основой для вычисления CVSS и имеет следующий вид (версия 2.10):

$$\text{Base Score} = \text{round_to_1_decimal}(((0.6 * \text{Impact}) + (0.4 * \text{Exploitability}) - 1.5) * f(\text{Impact}))$$

$$\text{Impact} = 10.41 * (1 - (1 - \text{ConfImpact}) * (1 - \text{IntegImpact}) * (1 - \text{AvailImpact}))$$

$$\text{Exploitability} = 20 * \text{Access Vector} * \text{Access Complexity} * \text{Authentication}$$

$$f(\text{Impact}) = 0 \text{ if Impact}=0,$$

$$1.176 \text{ otherwise}$$

Access Vector = case Access Vector of

requires local access: 0.395

adjacent network accessible: 0.646

network accessible: 1.0

Access Complexity = case Access Complexity of

high: 0.35

medium: 0.61

low: 0.71

Authentication = case Authentication of

requires multiple instances of authentication: 0.45

requires single instance of authentication: 0.56

requires no authentication: 0.704

Conf_Impact = case Confidentiality Impact of

none: 0.000

partial: 0.275

complete: 0.660

Integ_Impact = case Integrity Impact of

none: 0.000

partial: 0.275

complete: 0.660

Avail_Impact = case Availability Impact of

none: 0.000

partial: 0.275

complete: 0.660



Временная формула CVSS 2.0

При использовании временной формулы временные показатели объединяются с базовой оценкой, и получается временная оценка, находящаяся в пределах от 0 до 10. Кроме того, полученная по этой формуле временная оценка не превышает базовую и не более чем на 33% меньше ее. Временная формула имеет следующий вид:

TemporalScore =

round_to_1_decimal (BaseScore*Exploitability*RemediationLevel*ReportConfidence)

Exploitability = case Exploitability of

unproven: 0.85

proof-of-concept: 0.90

functional: 0.95

high: 1.00

not defined: 1.00

Remediation Level = case Remediation Level of

official-fix: 0.87

temporary-fix: 0.90

workaround: 0.95

unavailable: 1.00

not defined: 1.00

Report Confidence = case Report Confidence of

unconfirmed: 0.90

uncorroborated: 0.95

confirmed: 1.00

not defined: 1.00



Формула среды CVSS 2.0

При использовании формулы среды показатели среды объединяются с временной оценкой, и получается оценка среды, находящаяся в пределах от 0 до 10. Кроме того, полученная по этой формуле оценка не превышает временную оценку. Формула среды имеет следующий вид:

Environmental Score = round_to_1_decimal((Adjusted Temporal+(10 Adjusted Temporal)*Collateral Damage Potential)*Target Distribution)

Adjusted Temporal = Temporal Score recomputed with the Base Scores Impact sub-equation replaced with the Adjusted Impact equation

Adjusted Impact = min(10,10.41*(1-(1-ConflImpact*Conf_Req)*(1-IntegImpact*Integ_Req)*(1-AvailImpact*Avail_Req)))

Collateral Damage Potential = case Collateral Damage Potential of

none: 0.0

low: 0.1

low-medium: 0.3

medium-high: 0.4

high: 0.5

not defined: 0.0

Target Distribution = case Target Distribution of

none: 0.00

low: 0.25

medium: 0.75

high: 1.00

not defined: 1.00

Conf_Req = case Conf_Req (Integ_Req ,Avail_Req) of

low: 0.5

medium: 1.0

high: 1.51

not defined: 1.0



Методика оценки рисков



Базовый вектор

Итак, поговорим о базовом векторе [*base vector*]. Он записывается в следующем формате:

AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]

Это сокращенная запись уязвимости, в которой информация о метриках приводится вместе со значениями метрик. В скобках указываются возможные значения для указанных базовых метрик. Специалист по оценке выбирает одно значение для каждой базовой метрики.

Оценка

Формулы расчета базовой оценки [*base score*], возможности эксплуатации и элементов оценки воздействия приведены в в руководстве *A complete Guide to the Common Vulnerability Scoring System Version 2.0*. Калькулятор оценки уязвимостей : <https://nvd.nist.gov/cvss.cfm?calculator&version=2>

Уровень опасности

Базовая оценка зависит от оценки возможности эксплуатации и элементов оценок воздействия на систему и выставляется от 0 до 10, где 10 соответствует высочайшему уровню опасности уязвимости.

Система CVSS 2.0 не переводит оценку в уровень опасности. Для получения информации об уровне опасности можно, например, использовать шкалу опасности, разработанную центром [FortiGuard](#):



Методика оценки рисков



Уровень опасности FortiGuard

Критический	9 – 10
Высокий	7 – 8.9
Средний	4 – 6.9
Низкий	0.1 – 3.9
Информационный	0

Оценка по CVSS 2.0

Пример: Уязвимость в веб-приложении

Уязвимость, позволяющая атаку типа «подделка межсайтовых запросов» [cross-site request forgery] в панели администратора, позволяет добавить нового пользователя, удалить имеющегося пользователя или вообще всех пользователей.

Анализ базовых метрик и получение базового вектора:

Вектор доступа (AV): сетевой (N)

Сложность доступа (AC): средняя (M)

Аутентификация (Au): нулевая (N)

Воздействие на конфиденциальность (C): нулевое (N)

Воздействие на целостность (I): частичное (P)

Воздействие на доступность (A): полное (C)

Базовый вектор (AV:N/AC:M/Au:N/C:N/I:P/A:C)



Методика оценки рисков



Уровень опасности FortiGuard

Критический	9 – 10
Высокий	7 – 8.9
Средний	4 – 6.9
Низкий	0.1 – 3.9
Информационный	0

Оценка по CVSS 2.0

Пример: Уязвимость в веб-приложении

Базовый вектор (AV:N/AC:M/Au:N/C:N/I:P/A:C)

Пояснение: Для эксплуатации уязвимости администратор должен посетить вебсайт злоумышленника. Этим объясняется «средний» уровень сложности доступа. Вебсайт злоумышленника находится где-то в Интернете. Значит вектор доступа – сетевой. Для эксплуатации уязвимости не требуется аутентификации (администратору нужно только зайти на вебсайт злоумышленника). Злоумышленник может удалить всех пользователей, тем самым вызвав для них отказ системы в обслуживании. Именно поэтому воздействие уязвимости на доступность системы будет полным. Удаление всех пользователей еще не значит удаление всех данных в системе. Поэтому воздействие на целостность — частичное. Наконец, воздействие на конфиденциальность нулевое, т.к. добавленный пользователь по умолчанию прав на чтение не имеет. Калькулятор: *Common Vulnerability Scoring System Version 2 Calculator* для подсчета элементов оценок (из элементов возможности эксплуатации и воздействия) и базовой оценки:

Оценка возможности эксплуатации [*exploitability subscore*]: 8.6

Оценка элементов воздействия: 7.8

Базовая оценка: 7.8

Уровень опасности по FortiGuard Высокий



Методика оценки рисков версия 3.0 (2016)

Базовые метрики

Группа Common Vulnerability Scoring System-Special Interest Group (CVSS-SIG)
Проект Forum of Incident Response and Security Teams (FIRST)



Компоненты системы, для которых рассчитываются метрики:

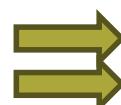
уязвимый компонент (vulnerable component) — тот компонент информационной системы, который содержит уязвимость и подвержен эксплуатации;

атакуемый компонент (impacted component) — тот, конфиденциальность, целостность и доступность которого могут пострадать при успешной реализации атаки.

В большинстве случаев **уязвимый** и **атакуемый** компоненты совпадают, но есть целые классы уязвимостей, для которых это не так, например:

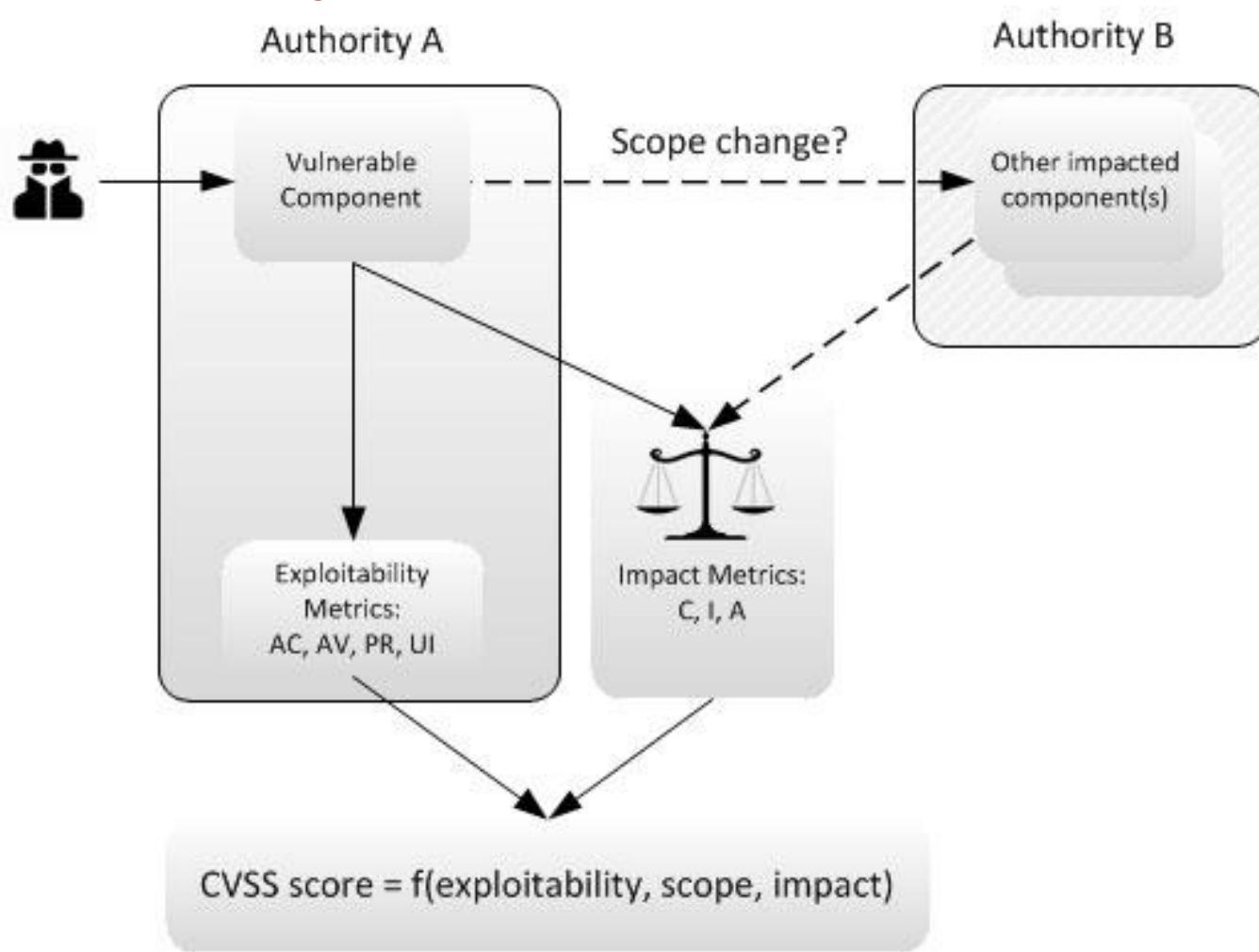
- выход за пределы песочницы приложения;
- получение доступа к пользовательским данным, сохраненным в браузере, через уязвимость в веб-приложении (XSS);
- выход за пределы гостевой виртуальной машины.

CVSS v 3: **Метрики эксплуатируемости**
Метрики воздействия



для **уязвимого компонента**
для **атакуемого компонента**

Границы, Уязвимый компонент, Атакуемый компонент



Методика оценки рисков версия 3.0



Метрики эксплуатируемости

Вектор атаки

БАЗОВЫЕ МЕТРИКИ

CVSS v 2.0	CVSS v 3.0:
Название метрики: Вектор атаки	
Access Vector (AV)	Attack Vector (AV)
Возможные значения метрики	
Network (N)	Network (N)
Adjacent Network (A)	Adjacent Network (A)
Local (L)	Local (L)
	Physical (P)

- * **Local** — для эксплуатации атакующему требуется локальная сессия или определенные действия со стороны легитимного пользователя.
- * **Physical** — атакующему требуется физический доступ к уязвимой подсистеме.

Методика оценки рисков версия 3.0



Вектор атаки Attack Vector

Значение показателя	Описание
Сетевой (Network, N)	<p>В случае уязвимости, эксплуатация которой возможна при доступе через сеть, уязвимый компонент привязан к сетевому стеку, а маршрут проникновения злоумышленника пролегает через уровень 3 (сетевой уровень) модели взаимосвязи открытых систем (OSI). Такие уязвимости часто называются "уязвимостями с возможностью дистанционной эксплуатации", то есть эксплуатации через один или несколько сетевых пролетов (например, через границы уровня 3 с маршрутизаторов). Примером сетевой атаки может служить инициирование злоумышленником отказа в обслуживании (DoS путем передачи особым образом сформированного TCP-пакета через общедоступный интернет (например, CVE-2004-0230)</p>
Соседский (Adjacent, A)	<p>В случае уязвимости, эксплуатация которой возможна со стороны соседей по сети, уязвимый компонент также привязан к сетевому стеку, но атака ограничена той же совместно используемой физической (например, Bluetooth, IEEE 802.11) или логической (например, локальной IP-подсетью) сетью и не может быть произведена через границы уровня 3 модели OSI (например, маршрутизатор). Примером "соседской" атаки является флуд-атака по протоколу разрешения адресов (ARP) (IPv4) или протоколу обнаружения соседей (IPv6), вызывающая отказ в обслуживании в местном сегменте локальной вычислительной сети (ЛВС). См. также CVE-2013-6014</p>

Методика оценки рисков версия 3.0



Вектор атаки Attack Vector

Значение показателя	Описание
Локальный (Local, L)	<p>В случае уязвимости, которая может эксплуатироваться при локальном доступе, уязвимый компонент не привязан к сетевому стеку, а маршрут проникновения злоумышленника пролегает через возможности чтения/записи/выполнения. В одних случаях злоумышленник эксплуатирует уязвимость, войдя локально в систему, в других он/она может полагаться на взаимодействие с пользователем (UI) для выполнения вредоносного файла</p>
Физический (Physical, P)	<p>В случае уязвимости, которая может эксплуатироваться при физическом доступе, злоумышленнику для достижения своей цели необходимо физическое взаимодействие с уязвимым компонентом. Это физическое взаимодействие может быть кратковременным (как, например, при атаке типа Evil maid1) или постоянным. Примерами такой атаки могут служить атака методом холодной перезагрузки, позволяющая злоумышленнику получить доступ к ключам шифрования диска после получения физического доступа к системе, или атаки с прямым доступом в память через периферийные устройства Firewire/USB</p>

Методика оценки рисков версия 3.0



Вектор атаки: ПРИМЕР

Рассмотрим две уязвимости, имеющие одинаковую оценку с точки зрения

CVSSv2.0: 7.2

AV:L /AC:L /Au:N /C:C /I:C /A:C

CVE-2015-2363 — Драйвер *win32k.sys* операционной системы *Windows* некорректно обрабатывает ряд объектов в памяти, что позволяет злоумышленнику, имеющему локальный доступ к системе, получить административные привилегии и выполнить произвольный код в режиме ядра.

CVE-2015-3007 — Сетевые шлюзы *Juniper* серии *SRX* некорректно реализуют функцию отключения восстановления пароля непrivилегированным пользователем через консольный порт (*set system ports console insecure*). Уязвимость позволяет злоумышленнику, имеющему физический доступ к консольному порту, получить административные привилегии на устройстве.

Уязвимость	Вектор CVSSv3	Оценка CVSSv3
<u>CVE-2015-2363</u>	<u>AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</u>	7.8
<u>CVE-2015-3007</u>	<u>AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</u>	6.8

Методика оценки рисков версия 3.0



Метрики эксплуатируемости

Сложность эксплуатации уязвимости

БАЗОВЫЕ МЕТРИКИ

<i>CVSS v 2.0</i>	<i>CVSS v 3.0:</i>
Название метрики: Сложность эксплуатации уязвимости	
Access Complexity (AC)	Attack Complexity (AC) User Interaction (UI)
Возможные значения метрики	
Low (L)	Low (L)
Medium (M)	
High (H)	High (H)

* Факторы, учитываемые в CVSS v2.0 метрикой Access Complexity, в новом стандарте учитываются двумя метриками — Attack Complexity и User Interaction.

Методика оценки рисков версия 3.0



Вектор атаки Attack Complexity

Значение показателя	Описание
Низкая (Low, L)	<p>Не существует специальных условий доступа и особых обстоятельств. Злоумышленник может рассчитывать на успешное повторение атаки в отношении уязвимого компонента.</p>
Высокая (High, H)	<p>Успех атаки зависит от условий, находящихся вне контроля злоумышленника. Иными словами, успешная атака не может быть выполнена произвольно, а требует от злоумышленника приложения заметных усилий для подготовки или реализации такой атаки в отношении уязвимого компонента 2. Например, успех атаки может зависеть от любого из следующих условий:</p> <ul style="list-style-type: none"> - злоумышленник должен собрать некоторую информацию о целевом объекте атаки – например, о настройках конфигурации, порядковых номерах, совместно используемых секретных ключах и т. д.; - злоумышленник должен подготовить целевую среду для повышения надежности эксплуатации – например, для повторной эксплуатации, нацеленной на получение выигрышного результата в условиях состязания, или для преодоления прогрессивных методов защиты от эксплуатации; <input type="checkbox"/> - злоумышленник должен расположиться на логическом сетевом пути между целевым объектом и ресурсом, который был запрошен этим объектом, для чтения и/или изменения передаваемых по сети данных (например, атака через посредника).

Методика оценки рисков версия 3.0



Метрики эксплуатируемости

Сложность эксплуатации уязвимости: ПРИМЕР

Для уязвимостей, позволяющих реализовать атаку «Человек посередине», в базе NVD можно встретить различные варианты оценки Access Complexity.

CVE-2014-2993 — Уязвимость в функции проверки SSL-сертификата приложения *Birebin.com* для операционной системы *Android* позволяет злоумышленнику осуществить атаку «Человек посередине» и получить доступ к конфиденциальным данным. **[Access Complexity — Low]**

CVE-2014-3908 — Уязвимость в функции проверки SSL-сертификата приложения *Amazon.com Kindle* для операционной системы *Android* позволяет злоумышленнику осуществить атаку «Человек посередине» и получить доступ к конфиденциальным данным. **[Access Complexity — Medium]**

CVE-2014-5239 — Уязвимость в функции проверки SSL-сертификата приложения *Microsoft Outlook.com* для операционной системы *Android* позволяет злоумышленнику осуществить атаку «Человек посередине» и получить доступ к конфиденциальным данным. **[Access Complexity — High]**

*CVSS 3.0 Уязвимости (атаки «Человек посередине») – только **High**

Методика оценки рисков версия 3.0



Метрики эксплуатируемости

Аутентификация / требуемый уровень привилегий
(Privileges Required, PR)

БАЗОВЫЕ МЕТРИКИ

CVSS v 2.0	CVSS v 3.0:
Название метрики: Требуемый уровень привилегий	
Authentication (Au)	Privileges Required (PR)
Возможные значения метрики	
Multiple (M)	
Single (S)	High (H) Low (L)
None (N)	None (N)

Методика оценки рисков версия 3.0



Метрики эксплуатируемости

Аутентификация / требуемый уровень привилегий: ПРИМЕР

* Значение **Multiple** в базе NVD встречается достаточно редко и в основном используется для уязвимостей, информация о которых недостаточно детализирована.

CVE-2015–0501 — Неизвестная уязвимость в Oracle MySQL Server позволяет удаленным аутентифицированным пользователям нарушить доступность СУБД, используя неизвестный вектор, связанный с «Server:Compiling».

* Значение **Single** не позволяет определить, требуется ли для эксплуатации доступ уровня привилегированного пользователя или достаточно аутентификации стандартного пользователя.

Методика оценки рисков версия 3.0



Метрики эксплуатируемости

Аутентификация / Требуемый уровень привилегий: ПРИМЕР

Рассмотрим две уязвимости, имеющие одинаковую оценку с точки зрения CVSSv2:

9.0 AV:N /AC:L /Au:S /C:C /I:C /A:C

CVE-2014-0649 — Cisco Secure Access Control System (ACS) некорректно выполняет авторизацию при доступе к интерфейсу Remote Method Invocation (RMI), что позволяет удаленным аутентифицированным злоумышленникам получить административные привилегии.

CVE-2014-9193 — Innominate mGuard некорректно обрабатывает настройки Point-to-Point Protocol (PPP), что позволяет удаленным злоумышленникам, имеющим ограниченные административные права, получить привилегии суперпользователя.

Уязвимость	Вектор CVSSv3	Оценка CVSSv3
<u>CVE-2014-0649</u>	<u>AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</u>	8.8
<u>CVE-2014-9193</u>	<u>AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</u>	7.2

* CVSSv3 занижает опасность уязвимостей, требующих для эксплуатации привилегированного доступа.

Методика оценки рисков версия 3.0



Метрики эксплуатируемости

Необходимость взаимодействия с пользователем

БАЗОВЫЕ МЕТРИКИ

CVSS v 2.0	CVSS v 3.0:
Название метрики: Необходимость взаимодействия с пользователем	User Interaction(UI)
Возможные значения метрики	
	None (N)
	Required (R)

* В CVSS v2.0 этот фактор учитывался в рамках метрики Access Complexity, в новом стандарте представлен в виде самостоятельной метрики.

Методика оценки рисков версия 3.0



Метрики эксплуатируемости

Необходимость взаимодействия с пользователем: ПРИМЕР

Рассмотрим две уязвимости, имеющие одинаковую оценку с точки зрения

CVSSv2: **9.3** AV:N /AC:M /Au:N /C:C /I:C /A:C

CVE-2014-0329 — Маршрутизаторы ZTE ZXV10 W300 имеют встроенную учетную запись администратора с фиксированным паролем формата «XXXXairocon', где XXXX — последние четыре символа MAC-адреса устройства. Удаленный атакующий может получить пароль администратора и использовать его для доступа к устройству через сервис Telnet.

CVE-2015-1752 — Microsoft Internet Explorer некорректно обрабатывает объекты в памяти, что позволяет атакующему выполнить произвольный код на системе при переходе пользователя по ссылке, содержащей вредоносный код.

Уязвимость	Вектор CVSSv3	Оценка CVSSv3
<u>CVE-2014-0329</u>	<u>AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</u>	9.8
<u>CVE-2015-1752</u>	<u>AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H</u>	8.8

Методика оценки рисков версия 3.0



Метрики эксплуатируемости

Границы эксплуатации: Scope

БАЗОВЫЕ МЕТРИКИ

CVSS v 2.0	CVSS v 3.0:
Название метрики: Границы эксплуатации	
	Scope (S)
Возможные значения метрики	
	Unchanged (U)
	Changed (C)

* Отличаются ли эксплуатируемый и атакуемый компоненты, то есть позволяет ли эксплуатация уязвимости нарушить конфиденциальность, целостность и доступность какого-либо другого компонента системы.

Методика оценки рисков версия 3.0



Метрики эксплуатируемости

Границы эксплуатации: ПРИМЕР

Рассмотрим две уязвимости, имеющие одинаковую оценку CVSSv2:

10.0 AV:N /AC:L /Au:N /C:C /I:C /A:C

CVE-2014-0568 — Уязвимость в обработчике системного вызова

NtSetInformationFile в Adobe Reader и Adobe Acrobat на операционной системе Windows позволяет атакующему обойти ограничения «песочницы» и выполнить произвольный код в привилегированном контексте.

CVE-2015-3048 — Уязвимость в Adobe Reader и Adobe Acrobat на операционных системах Windows и MacOS X позволяет атакующему вызвать переполнение буфера и выполнить произвольный код на системе.

Уязвимость	Вектор CVSSv3	Оценка CVSSv3
<u>CVE-2014-0568</u>	<u>AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H</u>	9.6
<u>CVE-2015-3048</u>	<u>AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H</u>	8.8

* Уязвимости, в которых уязвимый и атакуемый компоненты различаются, получают более высокую оценку опасности.

Методика оценки рисков версия 3.0



Метрики воздействия

Оценка степени влияния на конфиденциальность, целостность и доступность атакуемого компонента.

Воздействие на конфиденциальность, целостность, доступность

CVSS v 2.0	CVSS v 3.0:
Название метрики: Воздействие на CIA	
Confidentiality Impact (C), Integrity Impact (I), Availability Impact (A)	
Возможные значения метрики	
None (N)	None (N)
Partial (P)	
Complete (C)	Medium (M) High (H)

Методика оценки рисков версия 3.0



Метрики воздействия

Воздействие на конфиденциальность, целостность, доступность: ПРИМЕР

Рассмотрим две уязвимости, имеющие одинаковую оценку CVSSv2:

5.0 (AV: N/AC: L/Au: N/C: P/I: N/A: N).

CVE-2014-0160 — Уязвимость существует в реализации TLS и DTLS для OpenSSL из-за некорректной обработки пакетов расширения Heartbeat. Эксплуатация данной уязвимости позволяет злоумышленникам, действующим удаленно, получить доступ к конфиденциальной информации из памяти процесса при помощи специально сформированных пакетов, которые вызывают чтение за пределами буфера.

CVE-2015-4202 — Реализация Cable Modem Termination Systems (CMTS) в маршрутизаторах Cisco uBR10000 не дает возможность ограничить доступ к сервису IP Detail Record (IPDR), что позволяет удаленному атакующему получить доступ к конфиденциальной информации путем отсылки специально сформированных IPDR-пакетов.

Уязвимость	Вектор CVSSv3	Оценка CVSSv3
<u>CVE-2014-0160</u>	<u>AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N</u>	7.5
<u>CVE-2015-4202</u>	<u>AV:N/AC:L/PR:N/UI:N/S:U/C:M/I:N/A:N</u>	5.3

Методика оценки рисков версия 3.0



Степень зрелости доступных средств эксплуатации

Доступен ли публично код или другие средства, с помощью которых можно провести атаку, или, напротив, существует только теоретическая возможность эксплуатации.

CVSS v 2.0	CVSS v 3.0:
Название метрики: Степень зрелости	
Exploitability (E)	Exploit Code Maturity (E)
Возможные значения метрики	
Not Defined (ND/X)	
High (H)	
Functional (F)	
Proof-of-Concept (POC/P)	
Unproven (U)	

Методика оценки рисков версия 3.0



Доступные средства устранения уязвимости

Существуют ли официальные или неофициальные средства устранения уязвимости.

CVSS v 2.0	CVSS v 3.0:
Название метрики: Средства устранения уязвимости	
Remediation Level (RL)	Remediation Level (RL)
Возможные значения метрики	
	Not Defined (ND/X)
	Unavailable (U)
	Workaround (W)
	Temporary Fix (TF/T)
	Official Fix (OF/O)

Методика оценки рисков версия 3.0



Степень доверия к информации об уязвимости

Степень детализации доступных отчетов об уязвимости

CVSS v 2.0	CVSS v 3.0:
Название метрики: Доверие к инфо об уязвимости	
Report Confidence (RC)	Report Confidence (RC)
Возможные значения метрики	
Not Defined (ND/X)	
Unconfirmed (UC)	
Uncorroborated (UR)	Unknown (U) Reasonable (R)
Confirmed (C)	Confirmed (C)

Unknown — в существующих отчетах отсутствует описание причины уязвимости или различные исследователи расходятся относительно причин и возможных последствий эксплуатации;

Reasonable — существуют отчеты об уязвимости, позволяющие судить о причинах уязвимости с достаточной степенью уверенности (например, в отчете приводится пример эксплуатирующего кода);

Confirmed — уязвимость подтверждена производителем продукта или в свободном доступе находится полнофункциональный эксплойт.

Методика оценки рисков версия 3.0



Степень влияния временных метрик

Рассмотрим уязвимость:

CVE-2015-2373 — Уязвимость в сервисе Remote Desktop Protocol (RDP) операционной системы Windows позволяет удаленному атакующему выполнить произвольный код на системе путем отправки специально сформированных RDP-пакетов.

Версия стандарта	CVSS-вектор	Базовая оценка	Итоговая оценка
CVSSv2	AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C	10.0	7.4
CVSSv3	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	9.8	8.5

Стандарт CVSS v 3.0: формула расчета изменена в пользу снижения общего влияния временных метрик на итоговую числовую оценку.

Методика оценки рисков версия 3.0



Требования к безопасности

Позволяет задекларировать, какая характеристика данных атакуемого компонента (конфиденциальность, целостность или доступность) наиболее влияет на функциональность бизнес-системы или в целом на бизнес-процессы.

CVSS v 2.0	CVSS v 3.0:
	Название метрики:
	Confidentiality Requirement (CR), Integrity Requirement (IR), Availability Requirement (AR)
	Возможные значения метрики
	Not Defined (ND/X) High (H) Medium (M) Low (L)

Методика оценки рисков версия 3.0



ЦЕПОЧКИ УЯЗВИМОСТЕЙ: Vulnerability Chaining

Эксплуатируя несколько уязвимостей последовательно, можно нанести значительно больший урон.

* Новый стандарт рекомендует использовать метрики CVSS и для описания цепочек уязвимостей, комбинируя характеристики эксплуатируемости одной уязвимости с метриками воздействия другой. <http://cwe.mitre.org/documents/glossary/#Chain>.

ПРИМЕР:

Уязвимость 1 — Локальное повышение привилегий, не требующее взаимодействия с пользователем.

Уязвимость 2 — Уязвимость, позволяющая удаленному неаутентифицированному атакующему модифицировать файлы уязвимого компонента. Уязвимость требует от пользователя выполнения каких-либо действий для успешной эксплуатации, например перехода по ссылке.

Уязвимость	Вектор CVSSv3	Оценка CVSSv3
Уязвимость 1	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	8.4
Уязвимость 2	AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N	4.3

* В случае если при эксплуатации уязвимости 2 возможно модифицировать файлы приложения так, чтобы это могло привести к эксплуатации уязвимости 1, — можно говорить о наличии цепочки уязвимостей со следующими характеристиками.

Цепочка уязвимостей	Вектор CVSSv3	Оценка CVSSv3
Уязвимость 2 —> Уязвимость 1	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8

Методика оценки рисков версия 3.0

Качественная шкала оценки опасности

За годы использования CVSSv2 в разных компаниях сложились разные подходы к выставлению качественного уровня опасности на базе метрики CVSS:

Nvd.nist.gov: 0—3.9 Low; 4.0—6.9 Medium; 7.0—10.0 High;

Tenable: 0—3.9 Low; 4.0—6.9 Medium; 7.0—9.9 High; 10.0 Critical;

Rapid 7: 0—3.9 Moderate; 4.0—7.9 Severe; 8.0—10.0 Critical.

Стандарт CVSS v3.0 рекомендует использовать следующую шкалу качественных оценок:

Количественная оценка	Качественная оценка
0	None
0.1—3.9	Low
4.0—6.9	Medium
7.0—8.9	High
9.0—10.0	Critical

Определение XML-схемы CVSS v3.0

Определение XML-схемы (XSD) для системы CVSS задает структуру XML-файла со значениями показателей CVSS.

Цель: хранить или передавать такие данные в формате XML.

XSD-файл доступен по адресу:
<https://www.first.org/cvss/cvss-v3.0.xsd>.

Формулы CVSS v3.0

Базовая оценка

Формула базовой оценки есть функция от формул частных оценок (ISC) воздействия и возможности эксплуатации.

Базовая оценка определяется следующим образом:

If ($Impact \text{ sub score} \leq 0$) 0 else,

Scope Unchanged (оценка не изменяется)

Roundup(Minimum [($Impact + Exploitability$), 10]);

Scope Changed (оценка изменяется)

*Roundup(Minimum [1,08 * ($Impact + Exploitability$), 10]).*

Функция Round up (округление) определяется как наименьшее значение, заданное с точностью до одного знака после запятой, большее или равное входному значению.

Например, Round up(4,02) = 4,1, а Round up(4,00) = 4,0.

Формулы CVSS v3.0

Частная оценка воздействия (ISC) определяется как:

$$\begin{aligned} \text{Scope Unchanged} & \quad 6,42 \times ISCBase ; \\ \text{Scope Changed} & \quad 7,52 \times [ISCBase - 0,029] - 3,25 \\ & \quad \times [ISCBase - 0,02]^{15}, \end{aligned}$$

где:

$$ISCBase = 1 - [(1 - ImpactConf) \times (1 - ImpactInteg) \times (1 - ImpactAvail)],$$

а частная оценка возможности эксплуатации определяется как:

$$8,22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction.$$

Формулы CVSS 3.0

Временная оценка (Temporal score) определяется следующим образом: $\text{Roundup}(\text{BaseScore} \times \text{ExploitCodeMaturity})$

Оценка среды (Environmental score) определяется следующим образом:

If (Modified Impact Sub score <= 0) 0 else,

If Modified Scope is Unchanged

Round up(Round up (Minimum [× (M.Impact + M.Exploitability), 10]) × Exploit Code Maturity × Remediation Level × Report Confidence);

If Modified Scope is Changed

*Round up(Round up (Minimum [1,08
× (M.Impact + M.Exploitability
× Exploit Code Maturity
× Remediation Level
× Report Confidence).)*

Формулы CVSS 3.0

Уточненная частная оценка воздействия определяется следующим образом:

If Modified Scope is Unchanged

$$6,42 \times [ISCModified];$$

If Modified Scope is Changed

$$7,52 \times [ISCModified - 0,029] - 3,25 \times [ISCModified - 0,02]^{15}$$

где:

$$ISCModified = Minimum [[1 - (1 - M. IConf \times CR) \times (1 - M. IInteg \times IR) \times (1 - M. IAvail \times AR)], 0,915].$$

Частная оценка возможности эксплуатации определяется как:

$$8,22 \times M. AttackVector \times M. AttackComplexity \times M. PrivilegeRequired \times M. UserInteraction.$$

Методика оценки рисков версия 3.0



РЕСУРСЫ ДЛЯ ИЗУЧЕНИЯ:

Спецификация CVSSv3: <https://www.first.org/cvss/specification-document>

Рекомендации по использованию CVSSv3: <https://www.first.org/cvss/user-guide>

Примеры расчета метрик по методике CVSSv3: <https://www.first.org/cvss/examples>

Калькулятор CVSSv3: <https://www.first.org/cvss/calculator/3.0>

База уязвимостей National Vulnerability Database: <https://nvd.nist.gov/home.cfm>

Спецификация CVSSv2: <https://www.first.org/cvss/v2/guide>

Калькулятор CVSSv2: <https://nvd.nist.gov/cvss.cfm?calculator&version=2>

Открытое письмо в FIRST о слабых сторонах CVSSv2
CVSS Implementation Guide от NIST

Рекомендации ITU по использованию CVSS: <https://www.itu.int/rec/T-REC-X.1521-201104-I>

Microsoft Security Center of Excellence.

Руководство по управлению рисками безопасности

Обзор содержания

Глава 1. Обзор руководства по управлению рисками безопасности

Глава 2. Обзор рекомендаций по управлению рисками безопасности

Глава 3. Обзор управления рисками безопасности

Глава 4. Оценка рисков

Глава 5. Поддержка принятия решений

Глава 6. Реализация контроля и оценка эффективности программы

Приложение А. Оперативная оценка рисков

Приложение Б. Типичные активы информационных систем

Приложение В. Типичные угрозы

Приложение Г. Уязвимости

Средства и шаблоны

Microsoft Security Center of Excellence.

Руководство по управлению рисками безопасности

Средства и шаблоны содержатся в файле установщика:

Windows Security Risk Management Guide Tools and Templates.msi

При запуске этого файла будет создана следующая папка.

\%USERPROFILE%\Мои документы\Security Risk Management Guide Tools and Templates.

В данную папку будут помещены следующие средства и шаблоны.

Шаблон **Data Gathering Template (SRMGTool1-Data Gathering Tool.doc)**. Данный шаблон можно использовать на этапе оценки рисков при обсуждениях, описанных в главе 4 «Оценка рисков».

Рабочий лист **Summary Level Risk Analysis (SRMGTool2-Summary Risk Level.xls)**. Данный файл представляет собой книгу Microsoft® Excel®, которая поможет организациям выполнить начальный этап анализа рисков — анализ общего уровня.

Рабочий лист **Detail Level Risk Analysis (SRMGTool3-Detailed Level Risk Prioritization.xls)**. Данный файл представляет собой книгу Excel, которая поможет организациям выполнить подробный анализ основных рисков, выявленных в процессе анализа общего уровня.

Sample Schedule (SRMGTool4-Sample Project Schedule.xls). Данный файл представляет собой книгу Excel с общим расписанием проекта для процесса управления рисками безопасности, предлагаемого корпорацией Майкрософт, и содержит этапы, шаги и задачи, рассматриваемые в этом руководстве.

Microsoft Security Center of Excellence.

Руководство по управлению рисками безопасности

Решение **Microsoft Operations Framework (MOF)** - рекомендации, позволяющие обеспечивать надежность, доступность, поддерживаемость и управляемость важных систем на основе продуктов и технологий Майкрософт. Предоставляемые MOF руководства поставляются в виде технических документов, руководств по использованию, средств оценки, рекомендаций, примеров реализации, шаблонов, средств поддержки и служб, позволяющих решать проблемы, которые возникают при работе сотрудников, а также при использовании процессов, технологий и элементов контроля в сложных, распределенных, гетерогенных ИТ-средах.

Дополнительные сведения о [MOF](http://www.microsoft.com/mof) см. по адресу www.microsoft.com/mof

Решение **Microsoft Solutions Framework (MSF)** помогает в выполнении планов действий, разработанных в ходе реализации процесса управления рисками безопасности, предлагаемого корпорацией Майкрософт.

MSF - последовательный подход к технологическим проектам, основанный на определенных наборах принципов, моделях, концепциях, руководствах, порядках действия и проверенных рекомендациях корпорации Майкрософт. Применение MSF помогает организациям реализовывать высококачественные технологические решения в заданные сроки и в пределах выделенного бюджета.

Дополнительные сведения о [MSF](http://www.microsoft.com/msf) см. по адресу www.microsoft.com/msf

Microsoft Security Center of Excellence.

Руководство по управлению рисками безопасности



Рис. 1: Четыре этапа процесса управления рисками безопасности, предлагаемого корпорацией Майкрософт

Microsoft Security Center of Excellence.

Руководство по управлению рисками безопасности

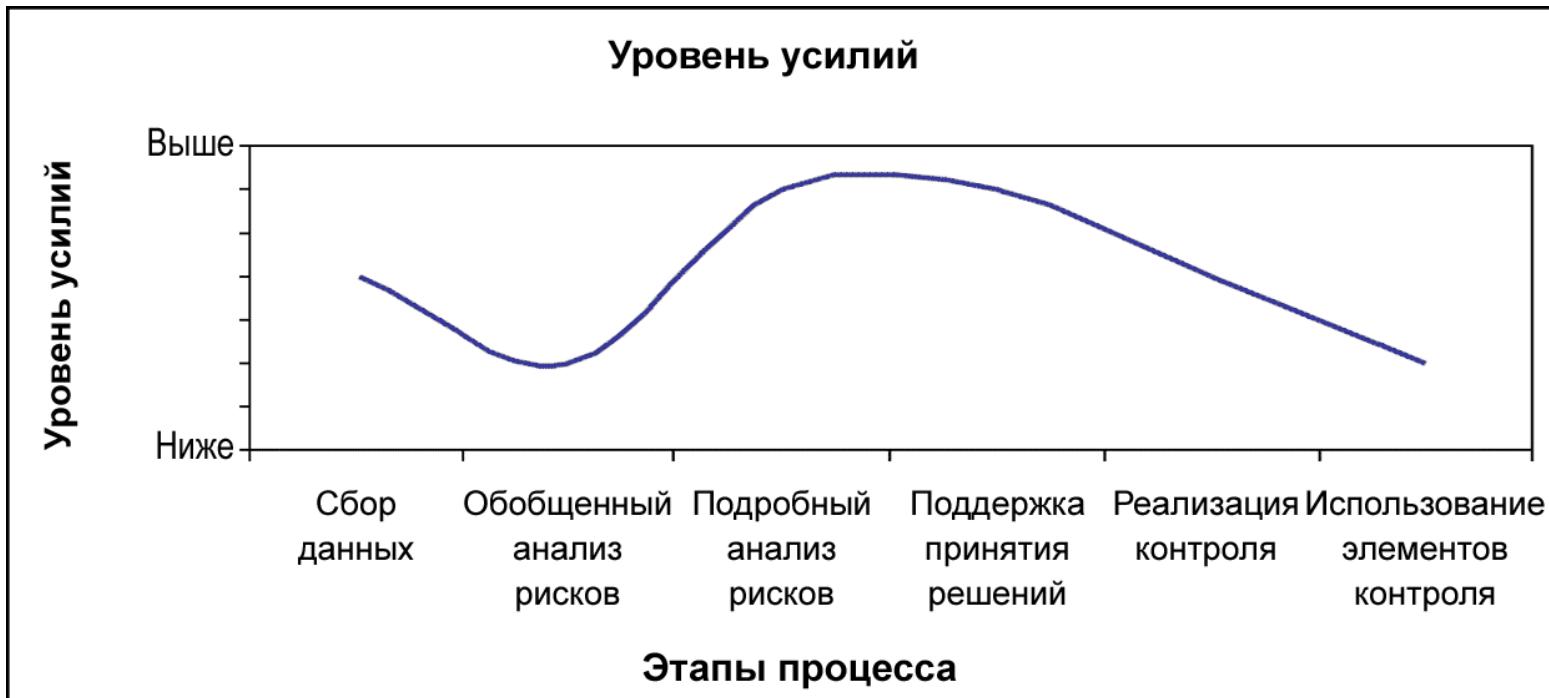


Рис. 2: Относительный уровень усилий в процессе управления рисками безопасности, предлагаемом корпорацией Майкрософт.

Дополнительные представления задач и соответствующих им усилий:
см. файл SRMGTool4-Sample Project Schedule.xls, в папке Tools и пример расписания проекта.

Microsoft Security Center of Excellence.

Руководство по управлению рисками безопасности



Рис. 3: Компоненты полной формулировки риска

* Риск — это вероятность того, что вследствие использования уязвимости в текущей среде пострадают конфиденциальность, целостность или доступность актива

Microsoft Security Center of Excellence.

Руководство по управлению рисками безопасности

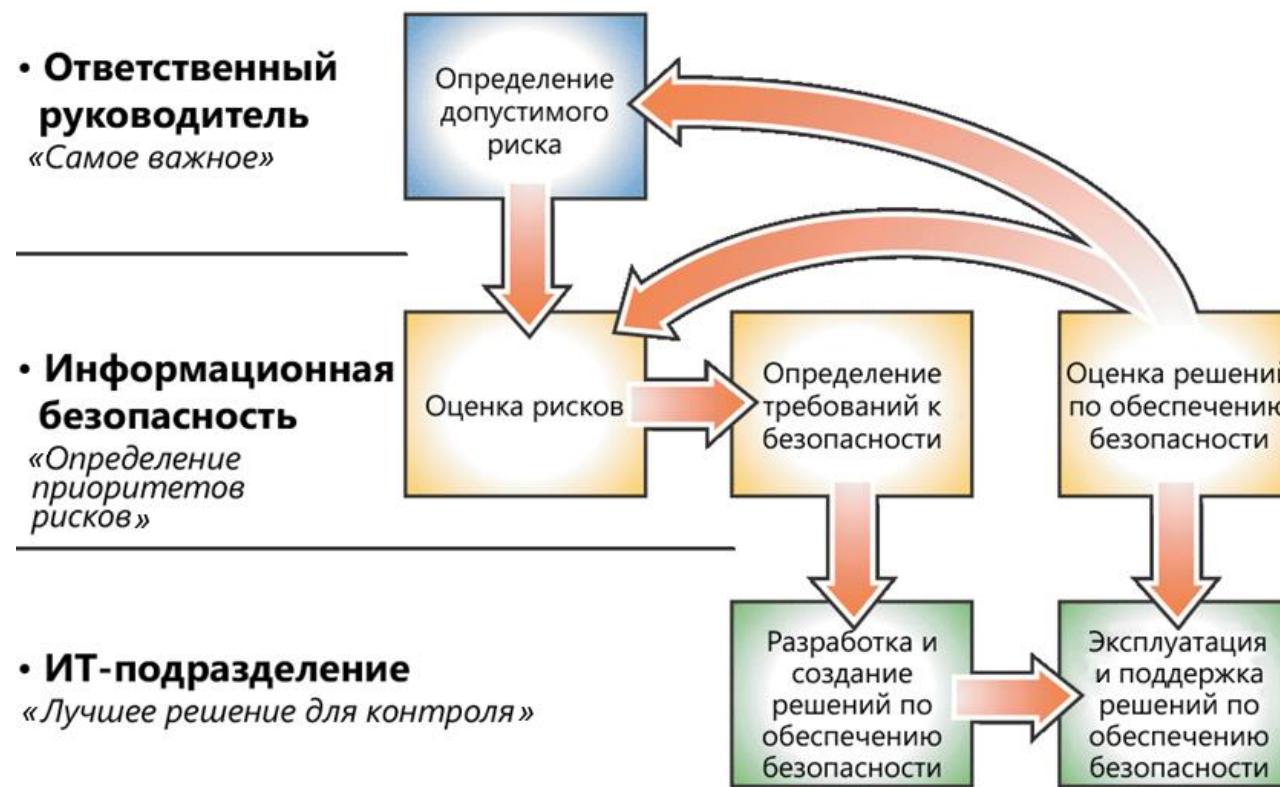


Рис. 4: Обзор основных ролей и обязанностей, используемых в процессе управления рисками безопасности, предлагаемом корпорацией Майкрософт

Microsoft Security Center of Excellence.

Руководство по управлению рисками безопасности

Как определить уровень зрелости организации?

Модель управления ИТ (IT Governance Maturity Model) описана в документе *CobiT (Control Objectives for Information and Related Technology)* института управления ИТ (ITGI).

Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, определения уровня зрелости основаны на стандарте Международной организации по стандартам (ISO) Information technology — Code of practice for information security management («Информационные технологии — практические правила управления информационной безопасностью»), называемом также ISO 17799.

Уровень	Состояние	Определение
0	Отсутствует	Политика или процесс не документированы. Ранее организация не знала о деловых рисках, связанных с управлением рисками, и не рассматривала данный вопрос
1	Узкоспециализированный	Некоторые члены организации признают значимость управления рисками, однако операции по управлению рисками являются узкоспециализированными. Политики и процессы в организации не документированы, процессы не являются полностью повторяемыми.
2	Повторяемый	Организации известно об управлении рисками. Процесс документирован не полностью, однако соответствующие операции выполняются регулярно, и организация стремится внедрить всеобъемлющий процесс управления рисками с привлечением высшего руководства. В организации не проводится формальное обучение и информирование по управлению рисками; ответственность за выполнение соответствующих мероприятий возложена на отдельных сотрудников
3	Наличие определенного процесса	Организация приняла формальное решение об интенсивном внедрении управления рисками для управления программой защиты информации. В организации разработан базовый процесс с четко определенными целями и задокументированными процессами достижения и оценки результатов. Проводится обучение всего персонала основам управления рисками. Организация активно внедряет задокументированные процессы управления рисками
4	Управляемый	На всех уровнях организации имеется глубокое понимание управления рисками. В организации существуют процедура управления рисками и четко определенный процесс, широко распространена информация об управлении рисками, доступно подробное обучение, существуют начальные формы измерений показателей эффективности. В организации используются некоторые технологические средства, помогающие в управлении рисками, однако большая часть (если не подавляющее большинство) процедур оценки рисков, определения элементов контроля и анализа выгод и затрат выполняется вручную
5	Оптимизированный	Организация выделила на управление рисками безопасности значительные ресурсы, а сотрудники пытаются прогнозировать, какие проблемы могут встретиться в течение следующих месяцев и лет и каким образом их нужно будет решать. Процесс управления рисками глубоко изучен и в значительной степени автоматизирован путем применения различных средств (разработанных в организации или приобретенных у сторонних разработчиков). При возникновении проблем в системе безопасности выявляется основная причина возникшей проблемы и предпринимаются необходимые действия для снижения риска ее повторного возникновения.

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

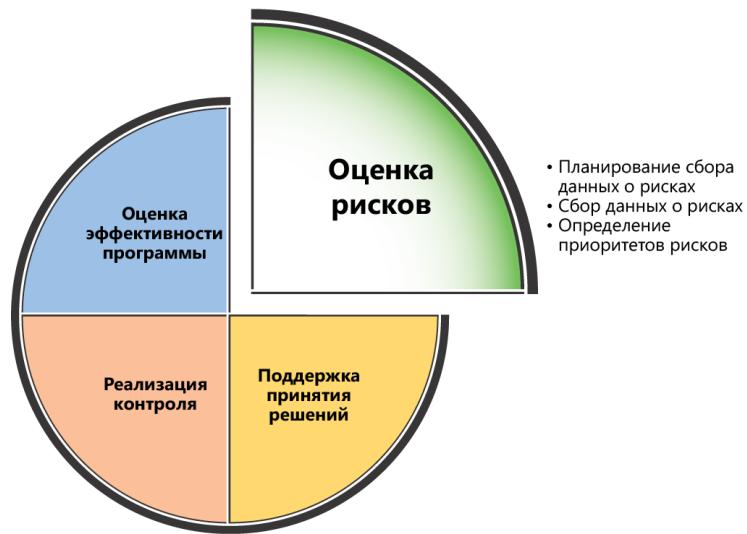


Рис. 5: Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт: этап оценки рисков.

Координированный сбор данных:

Активы организации. Вся информация о важных для организации активах.

Описание актива. Краткое описание каждого актива, его ценность и его владелец для облегчения общего понимания актива на этапе оценки рисков.

Угрозы безопасности. Причины и события, которые могут оказывать на актив негативное влияние и приводить к потере конфиденциальности, целостности или доступности актива.

Уязвимости. Слабости или отсутствие элементов контроля, которые могут использоваться для влияния на актив.

Текущая среда контроля. Описание используемых в настоящее время элементов контроля и их эффективности в рамках организации.

Предлагаемые элементы контроля. Предложения по снижения риска.

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Средства оценки рисков:

В процессе оценки рисков осуществляется сбор данных о рисках, а затем собранные данные используются для приоритизации рисков.

На этом этапе можно использовать следующие четыре средства, находящиеся в папке Tools and Templates, которая была создана при распаковке архива, содержащего данное руководство и сопутствующие файлы.

Шаблон Data Gathering Template (SRMGTool1-Data Gathering Tool.doc). Этот шаблон поможет проводить обсуждения при сборе данных о рисках.

Рабочий лист Summary Level Risk Analysis Worksheet (SRMGTool2-Summary Risk Level.xls). Данный рабочий лист Microsoft® Excel поможет организациям выполнить начальный этап анализа рисков — анализ общего уровня.

Рабочий лист Level Risk Analysis Worksheet (SRMGTool3-Detailed Level Risk Prioritization.xls). Данный рабочий лист Excel поможет организациям выполнить подробный анализ основных рисков, выявленных в процессе анализа общего уровня.

Примерное расписание Sample schedule (SRMGTool4-Sample Project Schedule.xls). Оно поможет в планировании операций для данного этапа.

Кроме того, в приложении Б «Типичные активы информационных систем» перечислены типичные активы информационных систем, встречающиеся в организациях различных типов.

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

КЛАССЫ АКТИВОВ:

Активами считается все, что представляет ценность для организации, включая как материальные активы (например, центры обработки данных, серверы и имущество, физическая инфраструктура), так и нематериальные (например, репутация организации, банковские транзакции, расчеты платежей, спецификации).

Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, определяет следующие три качественных класса активов:

высокое влияние на бизнес (ВВБ):

- Учетные данные. Например, пароли, секретные ключи шифрования и аппаратные маркеры.
- Конфиденциальные деловые данные. Например, финансовые данные и интеллектуальная собственность.
- Активы, к которым предъявляются особые регулятивные требования. Например, GLBA, HIPAA, CA SB1386 и директива ЕС о защите данных.
- Информация личного порядка (PII). Любые сведения, которые дают злоумышленнику возможность узнать информацию о заказчике или получить его личные данные.
- Данные авторизации финансовых транзакций. Такие как сроки действия и номера кредитных карт.
- Финансовые профили. Например, справки о кредитоспособности заказчиков и личные декларации о доходах.
- Медицинские профили. Например, номера медицинских карточек и биометрические данные.

среднее влияние на бизнес (СВБ):

- Внутренние коммерческие данные. Каталог сотрудников, данные о заказах на поставку, проекты сетевой инфраструктуры, данные, находящиеся на внутренних веб-узлах и во внутренних общих папках и предназначенные для использования только внутри организации.

низкое влияние на бизнес (НВБ):

- Общие сведения о структуре организации.
- Основные сведения о платформе, используемой для ИТ-операций.
- Возможность чтения общедоступных веб-страниц.
- Открытые ключи шифрования.
- Опубликованные пресс-релизы, брошюры с информацией о продуктах, информационные документы и документы, входящие в состав выпущенных продуктов.

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Упорядочивание по уровням многоуровневой защиты:



Оценка подверженности актива воздействию:

Высокая подверженность воздействию. Значительный или полный ущерб для актива.

Средняя подверженность воздействию. Средний или ограниченный ущерб.

Низкая подверженность воздействию.

Незначительный ущерб или отсутствие такового.

Оценка вероятности угроз:

Высокая. Вероятно возникновение одного или нескольких влияний в пределах года.

Средняя. Влияние может возникнуть в пределах двух-трех лет.

Низкая. Возникновение влияния в пределах трех лет маловероятно.

Рис. 6: Модель многоуровневой защиты

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Задача 1. Определение активов организации и сценариев:

Шаблон сбора данных, сведений о соответствующих материальных и нематериальных активах, а также активах ИТ-служб файл **SRMGTool1-Data Gathering Tool.doc**

Шаблон сбора данных

Определите активы, за разработку, поддержку, управление и сопровождение которых несет ответственность ваша группа

Название актива	Классификация актива (высокое, среднее или низкое влияние на деятельность)
1.	

Для каждого актива укажите следующие значения

Многоуровневая защита	Чего необходимо избежать (угрозы)	Пути возникновения (уязвимости)	Уровень подверженности воздействию (B, C, H)	Описания текущих элементов контроля	Вероятность (B, C, H)	Назначение контроля, потенциальные новые
Физический уровень						
Приложения						
Узлы						
Сеть						
Данные						

Рис. 7: Снимок экрана шаблона Data Gathering Template (SRMGTool1)

Задача 2. Выявление угроз

Задача 3. Выявление уязвимостей

Задача 4. Оценка подверженности актива воздействию

Задача 5. Выявление существующих элементов контроля и вероятности взлома

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

**Определение
влияния:**

Актив				Подверженность воздействию				
Дата обнаружения	Название актива	Класс актива	Применимые уровни многоуровневой защиты	Описание угрозы	Описание уязвимости	Уровень подверженности воздействию (B, C, H)	Уровень влияния (B, C, H)	
Дата	Информация о финансовых инвестициях заказчиков	BVB	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых компьютеров локальной сети вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	C	B	
Дата	Информация о финансовых инвестициях заказчиков	BVB	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых удаленных компьютеров вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	C	B	
Дата	Информация о финансовых инвестициях заказчиков	BVB	Данные	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных доверенным сотрудником с помощью подслушивания, методов социальной инженерии и других методов без использования технических средств	H	C	

Рис. 8: Рабочий лист Summary Risk Level Worksheet: столбцы Asset («Актив») и Exposure («Подверженность воздействию») (SRMGTool2)

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Приоритизация рисков безопасности

Задача 1. Определение величины влияния на основе формулировок влияний, полученных в процессе сбора данных

		Образец подверженности воздействию			
Класс актива	Выс.	Средн.	Выс.	Выс.	
	Средн.	Низк.	Средн.	Выс.	
	Низк.	Низк.	Низк.	Средн.	
	Низк.	Средн.	Выс.	Уровень подверженности воздействию	

Рис. 9: Рабочий лист анализа риска: класс актива и уровень подверженности воздействию (SRMGTool2)

Задача 2. Оценка вероятности влияния для перечня на обобщенном уровне

Высокая. Вероятно возникновение одного или нескольких влияний в течение года.

Средняя. Влияние может хотя бы один раз возникнуть в течение двух или трех лет.

Низкая. Возникновение влияния в течение трех лет маловероятно.

Задача 3. Завершение формирования перечня на обобщенном уровне путем объединения величин влияний и вероятностей для каждой формулировки риска

Уровни в списке с обобщенными сведениями о рисках					
Влияние (из предыдущей таблицы)	Выс.	Средн.	Выс.	Выс.	
	Средн.	Низк.	Средн.	Выс.	
	Низк.	Низк.	Низк.	Средн.	
	Низк.	Средн.	Выс.	Уровень вероятности	

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Приоритизация рисков безопасности

Информация, полученная в ходе процесса сбора данных						
Актив				Подверженность воздействию		
Дата обнаружения	Название актива	Класс актива	Применимые уровни многоуровневой защиты	Описание угрозы	Описание уязвимости	Уровень подверженности (B, C, H)
пример	Информация о финансовых инвестициях заказчиков	B2B	Узел	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых компьютеров локальной сети вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	
пример	Информация о финансовых инвестициях заказчиков	B2B	Узел	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых удаленных компьютеров вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	
пример	Информация о финансовых инвестициях заказчиков	B2B	Данные	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных доверенным сотрудником с помощью подслушивания, методов социальной инженерии и других методов без использования технических средств	

Уровень подверженности воздействию (B, C, H)	Уровень влияния (B, C, H)	Вероятность (B, C, H)	Обобщенный уровень риска (B, C, H)
Управляемые компьютеры с несвоевременным обновлением базовых средств или временной установки безопасности	C	B	C
Управляемые удаленные компьютеры с несвоевременным обновлением базовых средств или временной установки безопасности	C	B	B
Доверенным сотрудником с использованием социальной инженерии	H	C	H

Рис. 11: Рабочий лист анализа риска: перечень на обобщенном уровне (SRMGTool2)

На рис. 11 представлены все столбцы перечня на обобщенном уровне, который также включен в файл SRMGTool2-Summary Risk Level.xls

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Детализация рисков

Следующие четыре задачи дают общее представление о процессе составления перечня рисков на уровне детализации. Шаблон SRMGTool3-Detailed Level Risk Prioritization.xls в разделе Tools.

Результатом данного процесса является перечень на уровне детализации для рисков, влияющих на организацию. Количественная оценка вычисляется после подробного определения уровня риска и описывается в следующем разделе.

Задача 1. Определение величины влияния и подверженности воздействию

Уровень подверженности воздействию	Конфиденциальность или целостность актива
5	Серьезные повреждения или полный выход актива из строя (например, видимые снаружи и влияющие на прибыльность или успешность ведения бизнеса)
4	Серьезные повреждения, не приводящие к полному выходу актива из строя (например, влияющие на прибыльность или успешность ведения бизнеса и, возможно, видимые снаружи)
3	Средние повреждения или ущерб (например, влияющие на внутренние рекомендации по ведению бизнеса и способные вызвать увеличение эксплуатационных затрат или уменьшение доходов)
2	Незначительные повреждения или ущерб (например, влияющие на внутренние рекомендации по ведению бизнеса, но не вызывающие существенного роста затрат)
1	Небольшие изменения в активе или отсутствие изменений

Рис. 12: Рабочий лист анализа риска: уровни подверженности воздействию для конфиденциальности и целостности (SRMGTool3)

Уровень подверженности воздействию	Дата выпуска	Описание
5	Прекращение работы	Большие эксплуатационные затраты или нарушение коммерческих обязательств
4	Прерывание работы	Значительное увеличение эксплуатационных затрат или задержка при выполнении коммерческих обязательств
3	Задержки в работе	Заметное влияние на величину эксплуатационных затрат и производительность.
2	Отвлечение от работы	Измеримое влияние на деятельность компании отсутствует; небольшое увеличение эксплуатационных затрат или затрат на инфраструктуру
1	Не влияет на обычный ход бизнес-операций	Измеримое влияние на эксплуатационные затраты, производительность и коммерческие обязательства отсутствует

Рис. 13: Рабочий лист анализа риска: уровни подверженности воздействию для доступности (SRMGTool3)

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Детализация рисков

Следующие четыре задачи дают общее представление о процессе составления перечня рисков на уровне детализации. Шаблон SRMGTool3-Detailed Level Risk Prioritization.xls в разделе Tools.

Результатом данного процесса является перечень на уровне детализации для рисков, влияющих на организацию. Количественная оценка вычисляется после подробного определения уровня риска и описывается в следующем разделе.

Задача 1. Определение величины влияния и подверженности воздействию

Класс влияния	Значение класса влияния (3)
ВВБ	10
СВБ	5
НВБ	2

Уровень подверженности воздействию	Фактор подверженности воздействию (ФПВ)	Уровень влияния (3 * ФПВ)	Диапазон влияния	Обобщенное сравнение
5	100%		7 - 10	Выс.
4	80%		4 - 6	Средн.
3	60%		0 - 3	Низк.
2	40%			
1	20%			

Рис. 13: Рабочий лист анализа риска: определение величин влияния (SRMGTool3)

Актив	Подверженность воздействию						
	Название актива	Уровень класса влияния	Многоуровневая защита	Описание угрозы	Описание уязвимости	Уровень подверженности воздействию (1–5)	
Информация о финансовых инвестициях заказчиков	10 (ВВБ)	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых компьютеров локальной сети вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	4 (80%)	8	
Информация о финансовых инвестициях заказчиков	10 (ВВБ)	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых удаленных компьютеров вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	4 (80%)	8	

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Детализация рисков

Задача 2. Определение вероятности влияния

Целью данного процесса является создание целостного набора критериев оценки рисков в среде организации.

На рис. 14 используются следующие атрибуты уязвимостей:

Число злоумышленников. Как правило, вероятность взлома возрастает с увеличением числа злоумышленников и их квалификации.

Удаленный и локальный доступ. Как правило, возможность удаленного взлома увеличивает вероятность его успешности.

Известность средства взлома. Как правило, вероятность успешного взлома возрастает, если методы и средства взлома широко известны и общедоступны.

Автоматизация взлома. Как правило, вероятность успешного использования уязвимости возрастает, если средство взлома позволяет выполнять автоматический поиск уязвимостей в большой среде.

Определения вероятностей для уязвимостей	Результирующая оценка уязвимости
Высокая	
Большое число злоумышленников — любители и компьютерные хулиганы	
Удаленное выполнение	
Возможность использования анонимного доступа	
Общеизвестный метод взлома	
Автоматизированность	
5, если выполняется хотя бы одно из условий	
Средняя	
Среднее число злоумышленников — специалисты и эксперты	
Невозможность удаленного выполнения	
Необходимость наличия привилегий уровня пользователя	
Метод взлома не является общеизвестным	
Атака не автоматизирована	
3, если выполняется хотя бы одно из условий	
Низкая	
Небольшое число злоумышленников — необходима внутренняя информация	
Невозможность удаленного выполнения	
Необходимость наличия привилегий уровня администратора	
Метод взлома не является общеизвестным	
Атака не автоматизирована	
1, если выполняются все условия	
	Результирующая оценка уязвимости
	Атрибуты подверженности воздействию (выберите из числа указанных выше)
	высокая 5
	средняя 3
	низкая 1
	уровень вероятности (1, 3 или 5)
	Насколько эффективны текущие элементы контроля?
	Да — 0, Нет — 1
	Эффективно ли определена и реализована ответственность? 1,0
	Эффективно ли осуществляется информирование? 1,0
	Эффективно ли определены и реализованы процессы? 1,0
	Эффективно ли существующие технологии или элементы контроля снижают угрозы? 1,0
	Обеспечивают ли существующие методы аудита обнаружение злоупотреблений и недостатка контроля? 1,0
	Сумма атрибутов контроля (0–5) =

Рис. 14: Рабочий лист анализа риска: оценка уязвимости (SRMGTool3)

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Детализация рисков

Задача 3. Подробное определение уровня

Базовый риск (текущий)					
Актив		Подверженность воздействию			
Название актива	Уровень класса влияния	Многоуровневая защита	Описание угрозы	Описание уязвимости	Уровень подверженности воздействию
Описание влияния цифрового актива на деятельность	Уровень класса влияния (10, 5, 2)	Технические области, в которых проявляется подверженность воздействию: приложения, узлы, сеть, данные	Описание возможной угрозы или событий, которых необходимо избежать (например, изменения данных злоумышленником)	Описание путей возникновения угрозы (например, изменение данных злоумышленником путем внедрения отформатированной строки, которая будет исполнена как команда языка SQL)	Уровень подверженности воздействию
Риск (оценка)					
Уровень подверженности воздействию (1–5)	Уровень влияния (1–10)	Описания текущих элементов контроля	Уровень вероятности с контролем (1–10)	Уровень риска с контролем (0–100)	
Уровень подверженности воздействию (1–5) (SQL)	Уровень ущерба для актива, определяемый подверженностью воздействию	Люди, процессы и технологии, используемые в настоящее время для уменьшения вероятности влияния	Вероятность влияния на актив с текущими элементами контроля (см. определения уровней)	Общее влияние на деятельность организации с учетом актива и вероятности ущерба.	

Рис. 15: Рабочий лист анализа риска: подробное определение уровня риска (SRMGTool3)

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Детализация рисков

Задача 3. Подробное определение уровня

Базовый риск (текущий)									
Актив		Подверженность воздействию							
Название актива	Уровень класса влияния	Многоуровневая защита	Описание угрозы	Описание уязвимости	Уровень подверженности воздействию (1–5)	Уровень подверженности воздействию (1–10)	Описания текущих элементов контроля	Уровень вероятности с контролем (1–10)	Уровень риска с контролем (0–100)
Информация о финансовых инвестициях заказчиков	10 (ВВБ)	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых компьютеров локальной сети вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	4 (80%)	8	1. Каждый консультант имеет доступ только к информации о своих клиентах. Таким образом, подверженность воздействию составляет менее 100%. 2. Уведомления об обновлениях и исправлениях, отправляемые по электронной почте. 3. В локальной сети каждые несколько часов выполняется установка требуемых обновлений, что уменьшает временной интервал, в течение которого узлы локальной сети уязвимы перед взломом.	Уязвимость: Контроль: 1 Всего = 6	48
Информация о финансовых инвестициях заказчиков	10 (ВВБ)	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых удаленных компьютеров вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	4 (80%)	8	1. Каждый консультант имеет доступ только к информации о своих клиентах. Таким образом, подверженность воздействию составляет менее 100%. 2. Уведомления об обновлениях и исправлениях, отправляемые по электронной почте. — Отсутствует решение, позволяющее обеспечить соответствие требованиям за пределами локальной сети.	Контроль: 5 Всего = 10	80

Рис. 15: Пример банка : перечень рисков на уровне детализации (SRMGTool3)

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Детализация рисков

Задача 3. Подробное определение уровня

		Уровень влияния × Уровень вероятности = Уровень риска									
		Диапазоны вероятности									
		Диапазоны уровня влияния									
Выс.		10 -- 7			10 -- 7						
Средн.		6 -- 4			6 -- 4						
Низк.		3 -- 0			3 -- 0						

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Детализация рисков

Задача 4. Определение степени ожидаемого разового ущерба (ОРУ)

Величина высокого влияния на деятельность = \$ M		Уровень подверженности воздействию	Фактор подверженности воздействию, %
		5	100
Класс актива		4	80
Значение ВВБ	\$ M	3	60
Значение СВБ	\$ M/2	2	40
Значение НВБ	\$ M/4	1	20
Оценочное значение риска =	Значение класса актива × Фактор подверженности воздействию (%) = Ожидаемый разовый ущерб		

Рис. 17: Рабочий лист анализа риска: количественная оценка ожидаемого разового ущерба (SRMGTool3)

Описание риска	Значение класса актива	Уровень подверженности воздействию	Величина подверженности воздействию	Ожидаемый разовый ущерб
Риск для узла локальной сети	\$ 10	4	80%	\$ 8
Риск для удаленного узла	\$ 10	4	80%	\$ 8

Рис. 18: Определение ожидаемого разового ущерба в примере с банком : суммы указаны в миллионах долларов (SRMGTool3)

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Детализация рисков

Задача 5. Определение ежегодной частоты возникновения (ЕЧВ)

Качественный уровень	Описание	Диапазон ежегодной частоты возникновения	Примеры описаний
Высокий	Очень вероятно	≥ 1	Влияние раз в год или чаще
Средний	Вероятно	От 0,99 до 0,33	Не менее одного раза каждые 1–3 года
Низкий	Маловероятно	$< 0,33$	Реже, чем один раз в 3 года

Рис. 19: Количественная оценка ежегодной частоты возникновения (SRMGTool3)

Пример банка Группа управления рисками безопасности определила, что выбранные риски имеют следующие значения ЕЧВ.

ЕЧВ для узлов локальной сети. Используя качественную оценку среднего уровня вероятности, группа управления рисками безопасности определила, что данный риск может возникать один раз в два года или чаще. Таким образом, значение ЕЧВ равно 0,5.

ЕЧВ для удаленных узлов. Используя качественную оценку высокого уровня вероятности, группа управления рисками безопасности определила, что данный риск может возникать один раз в год или чаще. Таким образом, значение ЕЧВ равно 1.

Microsoft Security Center of Excellence.

Глава 4. Оценка рисков

Детализация рисков

Задача 6. Определение ожидаемого годового ущерба (ОГУ)

$$\text{Ожидаемый годовой ущерб (ОГУ)} = \text{ЕЧВ} \times \text{ОРУ}$$

Описание риска	Значение класса актива	Уровень подверженности воздействию	Величина подверженности воздействию	Ожидаемый разовый ущерб	Количественная оценка (ожидаемый годовой ущерб)	Количественная оценка (ожидаемый годовой ущерб)
Риск для узла локальной сети	\$ 10	4	80%	\$ 8	0,5	\$ 4
Риск для удаленного узла	\$ 10	4	80%	\$ 8	1	\$ 8

Рис. 20: Определение величины ожидаемого годового ущерба в примере с банком: суммы указаны в миллионах долларов (SRMGTool3)



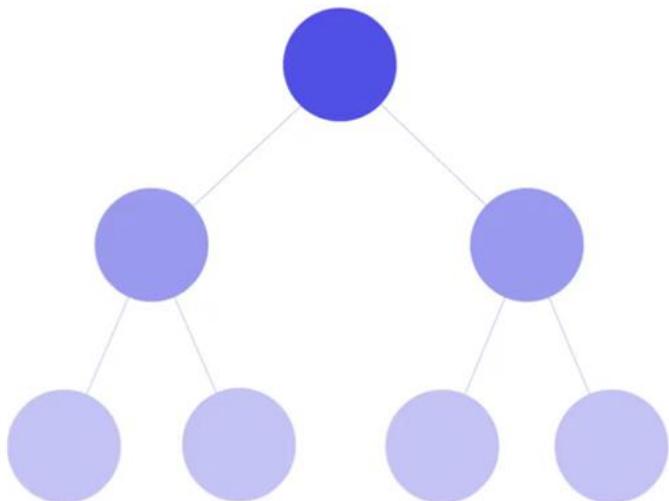
MITRE

CWE

cwe.mitre.org

Common Weakness Enumeration – CWE

Общая система оценки «слабых мест» программного обеспечения



Class

CWE-119: Improper Restriction of Operations whithin the Bounds of a Memory Buffer

Base

CWE-787: Out-of-Bounds Write

Variant

CWE-121: Stack-based Buffer Overflow

ОСНОВНЫЕ ПОНЯТИЯ CWE

Цель CWE состоит в том, чтобы обеспечить более эффективное обсуждение, описание, отбор и использование инструментальных средств и услуг по защите программного обеспечения, которые могут обнаруживать эти слабые места в кодах источников и операционных системах, а также улучшить понимание слабых мест программного обеспечения, связанных с его архитектурой и проектированием, и управление этими слабыми местами.

Перечень CWE предназначен для того, чтобы охватить причины всех общеизвестных видов уязвимости и незащищенности, связанных со слабыми местами в архитектуре, проектировании, кодировании или развертывании программного обеспечения.

Средство (capability) - инструментальное средство оценки, интегрированная среда разработки (IDE), средство смыслового анализа кода, компилирующая программа проверки кода, база данных, веб-сайт, инструкция или услуга, предоставляющая информацию о слабых местах на уровне внедрения, проектирования или архитектуры, способных привести к возникновению в таком программном обеспечении уязвимости в плане безопасности, которой могут воспользоваться.

Слабое место в системе информационной безопасности – это ошибка в программном обеспечении, вследствие которой может возникнуть уязвимость, которая может быть напрямую использована хакером для получения доступа в систему или сеть.

Слабое место (weakness) - дефект или изъян в коде, проектировании, архитектуре или развертывании программного обеспечения, способный в определенный момент стать уязвимостью или приводить к возникновению других уязвимостей.

Методики оценки

Приоретизация «Слабых Мест» на основе оценки бизнеса

The CWE project offers several approaches for prioritizing weaknesses so that you can focus on an appropriate subset for your organization's needs. Learn how to utilize these methods to benefit from the most improvement in the resilience, reliability, and integrity of your software as soon as possible.

Общая система оценки «слабых мест»

Common Weakness Scoring System (CWSS™)

CWSS provides a mechanism for scoring weaknesses in a consistent, flexible, open manner while accommodating context for various business domains. CWSS can also be used by individual developers to prioritize unfixed weaknesses within their own software.

Common Weakness Risk Analysis Framework (CWRAF™)

CWRAF, used in conjunction with CWSS, will provide your organization with a tailored "Top XX" list of common weaknesses.

CWE/SANS Top 25 Most Dangerous Software Errors

The CWE/SANS Top 25 Most Dangerous Software Errors is a periodically updated list of the most prevalent and easily exploited software common weaknesses as assessed by over 20 industry experts.

*SANS – Institute SysAdmin, Audit, Network, Security

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

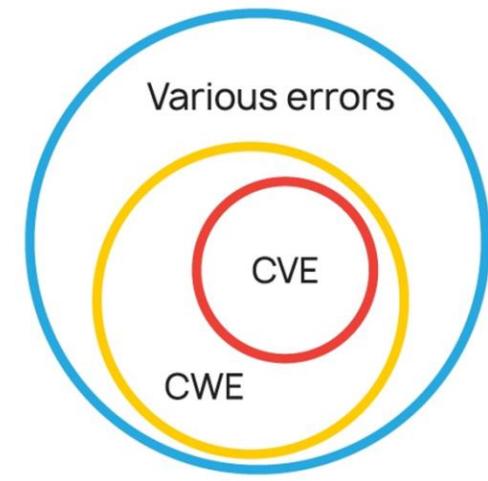
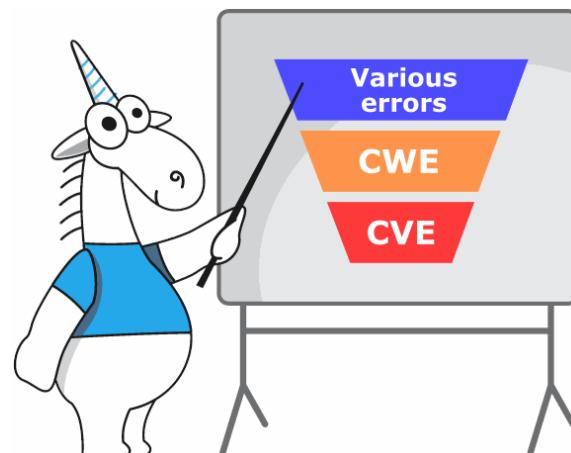


Rec. ITU-T X.1525 МСЭ-Т X.1525

В Рекомендации МСЭ-Т X.1525 по системе оценки общеизвестных слабых мест (CWSS) определена открытая структура представления информации о характеристиках и воздействиях слабых мест информационно-коммуникационных технологий (ИКТ) в ходе разработки возможностей программного обеспечения.

Цель этой Рекомендации состоит в том, чтобы предоставить разработчикам программного обеспечения ИКТ, руководителям в сфере ИКТ, испытателям, разработчикам средств защиты, поставщикам услуг, специалистам по закупкам и исследователям в области ИКТ возможность общаться, используя *общий язык оценки слабых мест ИКТ*, которые могут проявиться как уязвимости при использовании программного обеспечения.

<http://cwe.mitre.org/>



Таксономия системы CWE

Типе (тип) – это абстракция (метка) слабого места. Тип обозначается одним из шести символов:

V (variant) - Вариант - слабость, которая связана с определенным типом продукта, обычно с использованием определенного языка или технологии. Более конкретная, чем базовая слабость. Слабые стороны уровня варианта обычно описывают проблемы с точки зрения 3-5 следующих параметров: поведение, свойство, технология, язык и ресурс;

C (class) - Класс - это слабость, которая описывается очень абстрактно, как правило, независимо от какого-либо конкретного языка или технологии. Более конкретный, чем Pillar, но более общий, чем База. Слабые стороны уровня класса обычно описывают проблемы в терминах 1 или 2 следующих измерений: поведение, свойство и ресурс;

B (Base) - База - слабость, которая по-прежнему в основном не зависит от ресурса или технологии, но обладает достаточными деталями, чтобы предоставить конкретные методы обнаружения и предотвращения. Слабые стороны базового уровня обычно описывают проблемы в терминах 2 или 3 следующих параметров: поведение, свойство, технология, язык и ресурс;

Chain – Цепочка - сложный элемент, представляющий собой последовательность двух или более отдельных слабых мест, которые могут быть тесно связаны между собой в рамках программного обеспечения. Одна слабость, X, может непосредственно создать условия, необходимые для того, чтобы другая слабость, Y, вошла в уязвимое состояние. Когда это происходит, CWE обращается к X как к "первичному" Y, а Y является "результатирующим" от X. цепочки могут включать более двух слабых мест, и в некоторых случаях они могут иметь древовидную структуру.

P (Pillar) – слабость, которая является наиболее абстрактным типом слабости и представляет собой тему для всех слабостей класса / базы / варианта, связанных с ней.

Composite – Композит - сложный элемент, состоящий из двух или более различных слабых мест, в котором все слабые места должны присутствовать одновременно, чтобы возникла потенциальная уязвимость. Устранение любого из недостатков устраниет или резко снижает риск. Одна слабость, X, может быть "разбита" на составляющие слабости Y и Z. бывают случаи, когда одна слабость может не быть существенной для композита, но изменяет природу композита, когда он становится уязвимым.

Система CWE

CWE (Common Weakness Enumeration) - общий перечень уязвимостей и недостатков безопасности программного обеспечения (ПО), представляет собой иерархический словарь, предназначенный для разработчиков и специалистов по обеспечению безопасности ПО. CWE поддерживается MITRE по заказу Министерства внутренней безопасности США и развивается при широкой поддержке сообщества экспертов. По словам разработчиков, CWE — это общий язык для описания недостатков безопасности ПО, который необходим для стандартизации методик оценки программных продуктов с точки зрения информационной безопасности.

*Ошибки в программном обеспечении, которые могут быть непосредственно использованы злоумышленником для реализации угроз безопасности называют **уязвимостями**.
Ошибки, которые могут привести к возникновению уязвимостей – **недостатками безопасности**.*

Для классификации недостатков используется многоуровневая структура, которая описывает древовидное устройство CWE: конечные недостатки объединяются в типы, типы – в категории, категории – в представления. Каждое представление – особый способ классификации записей CWE, предназначенный для упрощения решения конкретной задачи.

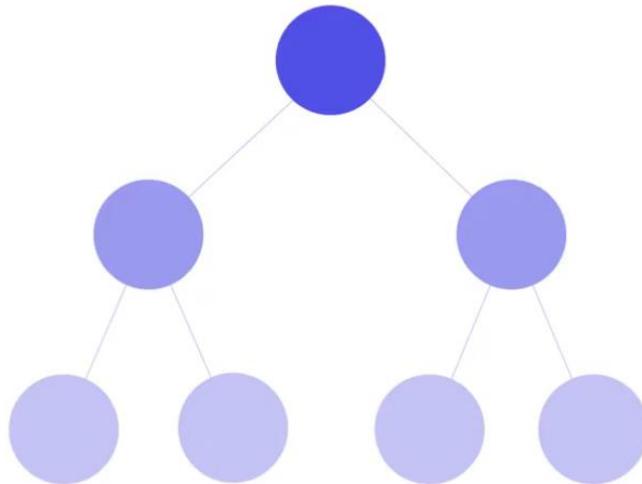
В последней версии три основных представления:

Концепции разработки – в этом представлении CWE недостатки безопасности классифицируются с использованием принципов и понятий, которые часто встречаются при разработке ПО; представление предназначено в первую очередь для разработчиков и специалистов по оценке качества ПО.

Концепции архитектуры – для анализа качества архитектурных решений на этапе проектирования.

Концепции исследований – представление, предназначенное для упрощения академических исследований. Отличается от первых двух высоким уровнем абстракций. Основное внимание в этом представлении удалено формальным понятиям поведения программного обеспечения, конкретные же примеры по возможности опускаются.

Таксономия системы CWE



Class

CWE-119: Improper Restriction of Operations whithin the Bounds of a Memory Buffer

Base

CWE-787: Out-of-Bounds Write

Variant

CWE-121: Stack-based Buffer Overflow

Buffer Errors

```
#include <String>
#define BUFSIZE 256

int main( int argc, char *argv[] )
{
    char *buffer1 = (char *) malloc(BUFSIZE);
    char *buffer2 = (char *) malloc(BUFSIZE);
    strcpy(buffer1, argv[1]);
    free(buffer2);
}
```

CWE-119

CWE Top 25 - 2023

Rank	ID	Name	Score	CVEs in KEV	Rank Change vs. 2022
1	CWE-787	Out-of-bounds Write	63.72	70	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.54	4	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	34.27	6	0
4	CWE-416	Use After Free	16.71	44	+3
5	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15.65	23	+1
6	CWE-20	Improper Input Validation	15.50	35	-2
7	CWE-125	Out-of-bounds Read	14.60	2	-2
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.11	16	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.73	0	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	10.41	5	0
11	CWE-862	Missing Authorization	6.90	0	+5
12	CWE-476	NULL Pointer Dereference	6.59	0	-1
13	CWE-287	Improper Authentication	6.39	10	+1
14	CWE-190	Integer Overflow or Wraparound	5.89	4	-1
15	CWE-502	Deserialization of Untrusted Data	5.56	14	-3
16	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	4.95	4	+1
17	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.75	7	+2
18	CWE-798	Use of Hard-coded Credentials	4.57	2	-3
19	CWE-918	Server-Side Request Forgery (SSRF)	4.56	16	+2
20	CWE-306	Missing Authentication for Critical Function	3.78	8	-2
21	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.53	8	+1
22	CWE-269	Improper Privilege Management	3.31	5	+7
23	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.30	6	+2
24	CWE-863	Incorrect Authorization	3.16	0	+4
25	CWE-276	Incorrect Default Permissions	3.16	0	-5

Алгоритм составления и ранжирования списка CWE Top 25

Основными источниками информации для исследования в этом году являлись:

- национальная база данных уязвимостей США (U.D. National Vulnerability Database (NVD)) за 2020–2021 годы;
- каталог эксплуатируемых уязвимостей (KEV) агентства по кибербезопасности и защите инфраструктуры США (Cybersecurity and Infrastructure Security Agency (CISA)), составленный в ноябре 2021 года.

Далее команда исследователей использует на полученных данных собственную формулу для расчёта порядка ранжирования, учитывающую частоту, с которой какой-либо недостаток (CWE) является основной причиной уязвимости, и потенциальную опасность эксплуатации. Частота и прогнозируемая серьёзность нормализованы относительно своих минимальных и максимальных значений.

Для вычисления частоты упоминания в формуле подсчитывается, сколько раз CVE ссылались на CWE в базе данных NVD. В расчёте используются только те CVE, которые имеют ссылку на CWE, поскольку использование полного набора данных привело бы к очень низким показателям частоты и незначительной разнице между различными типами дефектов.

$$Freq = \{count(CWE_X' \in NVD) \text{ for each } CWE_X' \text{ in } NVD\}$$

$$Fr(CWE_X) = (count(CWE_X \in NVD) - min(Freq)) / (max(Freq) - min(Freq))$$

Другим важным компонентом формулы ранжирования является расчёт серьёзности недостатка, который вычисляется по формуле:

$$Sv(CWE_X) = (average_CVSS_for_CWE_X - min(CVSS)) / (max(CVSS) - min(CVSS))$$

В конце вычисляется итоговая оценка путём перемножения оценки частоты упоминания на оценку серьёзности.

$$Score(CWE_X) = Fr(CWE_X) * Sv(CWE_X) * 100$$

Примеры CWE

Программные дефекты: переполнения буферов, ошибки форматной строки; проблемы структуры и валидации данных; манипуляции со специальными элементами; ошибки путей; проблемы с обработчиками; ошибки пользовательского интерфейса; проблемы обхода каталогов и распознавания эквивалентности путей; ошибки аутентификации; ошибки управления ресурсами; недостаточный уровень проверки данных; проблемы оценки входящих данных и внедрение кода; проблемы предсказуемости и недостаточная «случайность» случайных чисел;

Аппаратные дефекты: ошибки вычислений, обычно связанные с процессорами, графикой, компьютерным зрением (Vision), искусственным интеллектом (AI), ПЛИС (FPGA) и микроконтроллерами (uControllers); вопросы разделения привилегий и контроля доступа, относящиеся к идентификации, общим ресурсам, контролю блокировок и другим возможностям и механизмам; вопросы питания, работы часов, обработки напряжения, тока или температуры, контроля тактовой частоты и сохранения/восстановления состояния.

CWE List: структура и классификатор

[View by Software Development](#)

[View by Hardware Design](#)

[View by Research Concepts](#)

xternal groupings such as a Top-N list, as well as to express

[CWE Top 25 \(2020\)](#)

[OWASP Top Ten \(2017\)](#)

[Seven Pernicious Kingdoms](#)

[Software Fault Pattern Clusters](#)

[SEI CERT Oracle Coding Standard for Java](#)

[SEI CERT C Coding Standard](#)

[SEI CERT Perl Coding Standard](#)

[CISQ Quality Measures \(2020\)](#)

[Architectural Concepts](#)

[Introduced During Design](#)

[Introduced During Implementation](#)

[Quality Weaknesses with Indirect Security Impacts](#)

[Software Written in C](#)

[Software Written in C++](#)

[Software Written in Java](#)

[Software Written in PHP](#)

[Weaknesses in Mobile Applications](#)

[CWE Composites](#)

[CWE Named Chains](#)

[CWE Cross-Section](#)

[CWE Simplified Mapping](#)

[CWE Deprecated Entries](#)

[CWE Comprehensive View](#)

[Weaknesses without Software Fault Patterns](#)

[Weakness Base Elements](#)

CWE List: Software Development

ID:699

[Home](#) | [About](#) | [CWE List](#) | [Scoring](#) | [Community](#) | [News](#) | [Search](#)

CWE VIEW: Software Development

View ID: 699
Type: Graph

Status: Draft

Downloads: [Booklet](#) | [CSV](#) | [XML](#)

▼ Objective

This view organizes weaknesses around concepts that are frequently used or encountered in software development. This includes all aspects of the software development lifecycle including both architecture and implementation. Accordingly, this view can align closely with the perspectives of architects, developers, educators, and assessment vendors. It provides a variety of categories that are intended to simplify navigation, browsing, and mapping.

▼ Audience

Stakeholder	Description
Software Developers	Software developers (including architects, designers, coders, and testers) use this view to better understand potential mistakes that can be made in specific areas of their software application. The use of concepts that developers are familiar with makes it easier to navigate this view, and filtering by Modes of Introduction can enable focus on a specific phase of the development lifecycle.
Educators	Educators use this view to teach future developers about the types of mistakes that are commonly made within specific parts of a codebase.

▼ Relationships

The following graph shows the tree-like relationships between weaknesses that exist at different levels of abstraction. At the highest level, categories and pillars exist to group weaknesses. Categories (which are not technically weaknesses) are special CWE entries used to group weaknesses that share a common characteristic. Pillars are weaknesses that are described in the most abstract fashion. Below these top-level entries are weaknesses at varying levels of abstraction. Classes are still very abstract, typically independent of any specific language or technology. Base level weaknesses are used to present a more specific type of weakness. A variant is a weakness that is described at a very low level of detail, typically limited to a specific language or technology. A chain is a set of weaknesses that must be reachable consecutively in order to produce an exploitable vulnerability. While a composite is a set of weaknesses that must all be present simultaneously in order to produce an exploitable vulnerability.

Show Details:

[Expand All](#) | [Collapse All](#) | [Filter View](#)

699 - Software Development

- C API / Function Errors - (1228)
- C Audit / Logging Errors - (1210)

CWE List: Software Development

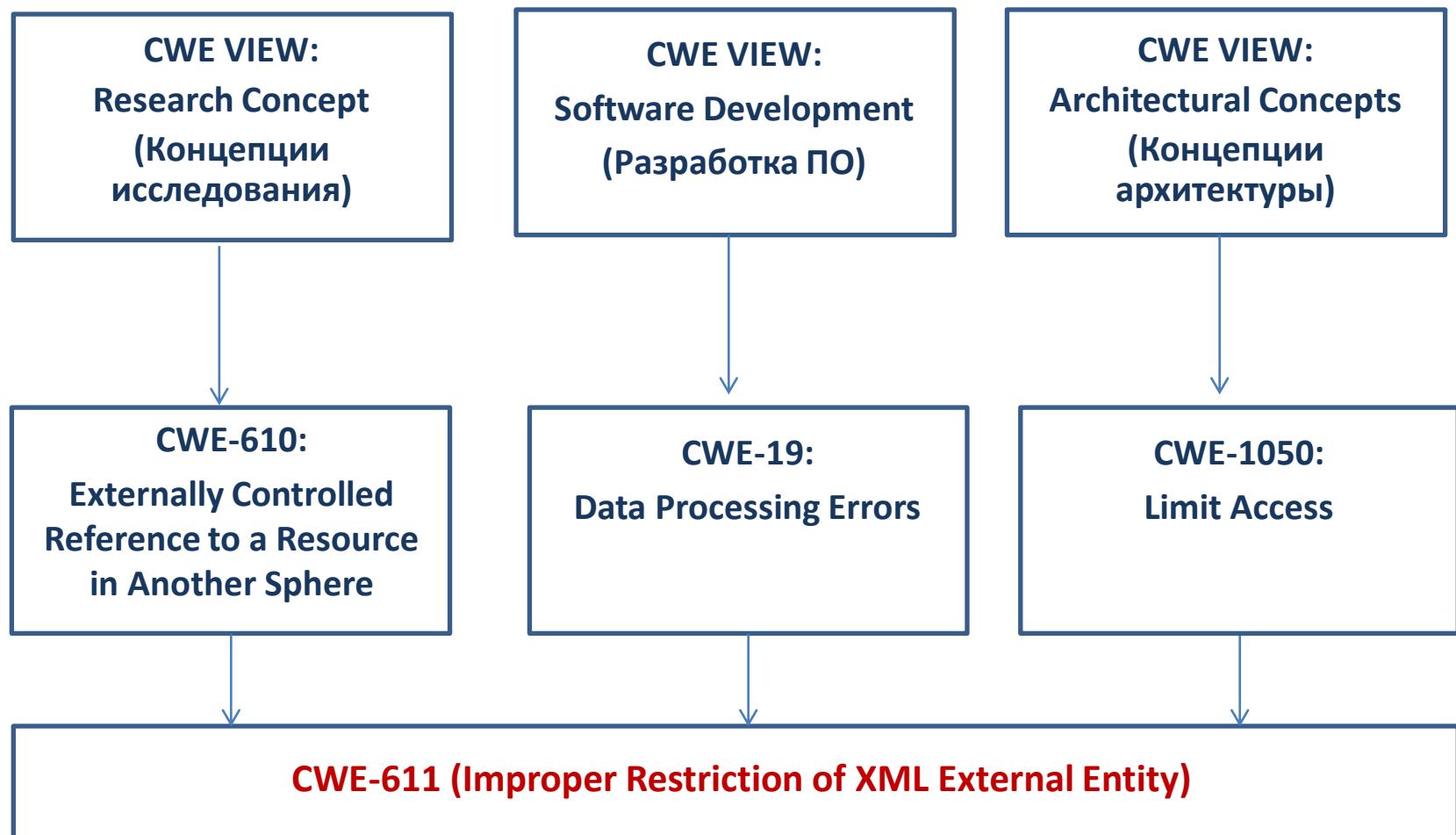
ID:699

699 - Software Development

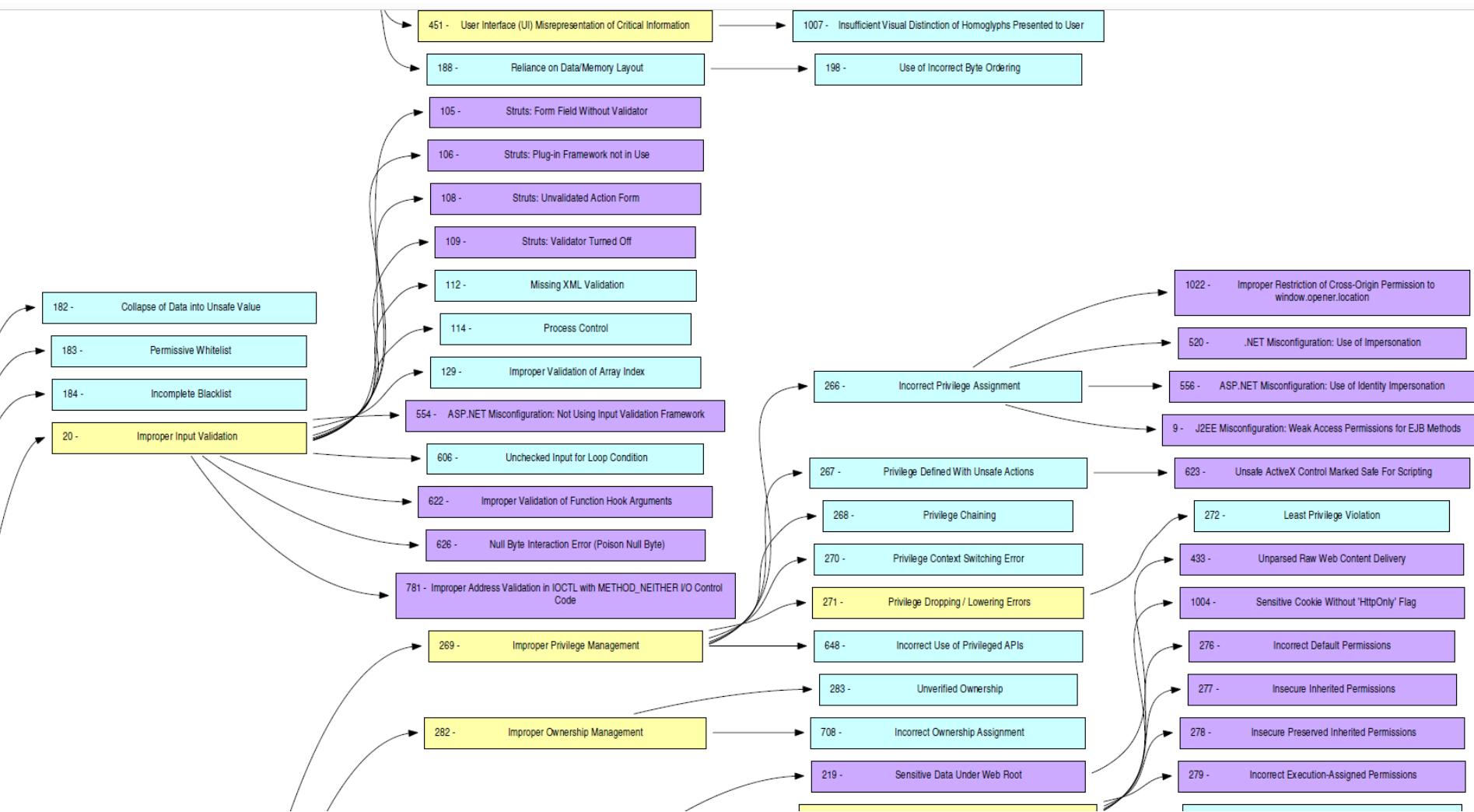
- **C** API / Function Errors - (1228)
 - . **B** Use of Inherently Dangerous Function - (242)
 - . **B** Use of Function with Inconsistent Implementations - (474)
 - . **B** Undefined Behavior for Input to API - (475)
 - . **B** Use of Obsolete Function - (477)
 - . **B** Use of Potentially Dangerous Function - (676)
 - . **B** Use of Low-Level Functionality - (695)
 - . **B** Exposed Dangerous Method or Function - (749)
- **C** Audit / Logging Errors - (1210)
- **C** Authentication Errors - (1211)
- **C** Authorization Errors - (1212)
- **C** Bad Coding Practices - (1006)
- **C** Behavioral Problems - (438)
- **C** Business Logic Errors - (840)
- **C** Communication Channel Errors - (417)
- **C** Complexity Issues - (1226)
- **C** Concurrency Issues - (557)
- **C** Credentials Management Errors - (255)
- **C** Cryptographic Issues - (310)
- **C** Key Management Errors - (320)
- **C** Data Integrity Issues - (1214)
- **C** Data Processing Errors - (19)

Пример таксономии CWE, граф связей

Уязвимость – **CVE-2010-2245** (внедрение внешних XML-сущностей в веб-сервисе Apache версии ниже 1.1.1) и недостаток безопасности **CWE-611** (неверное ограничение XML-ссылок на внешние объекты), послуживший причиной этой уязвимости.



Пример таксономии CWE, граф связей



<https://cwe.mitre.org/data/pdfs.html>

CWE List Version 4.9 содержит 934 идентифицированных слабых мест.

This section provides details for each individual CWE entry, along with links to additional information. See the [Organization of the Top 25](#) section for an explanation of the various fields.

1

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Summary

Weakness Prevalence	High	Consequences	Data loss, Security bypass
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

Discussion

These days, it seems as if software is all about the data: getting it into the database, pulling it from the database, massaging it into information, and sending it elsewhere for fun and profit. If attackers can influence the SQL that you use to communicate with your database, then suddenly all your fun and profit belongs to them. If you use SQL queries in security controls such as authentication, attackers could alter the logic of those queries to bypass security. They could modify the queries to steal, corrupt, or otherwise change your underlying data. They'll even steal data one byte at a time if they have to, and they have the patience and know-how to do so. In 2011, SQL injection was responsible for the compromises of many high-profile organizations, including Sony Pictures, PBS, MySQL.com, security company HBGary Federal, and many others.

Category-Based View of the Top 25

Категории «слабых мест»

Три категории «слабых мест» CWE/SANS Top 25:

- Insecure Interaction Between Components (Небезопасное взаимодействие между компонентами);
- Risky Resource Management (Рисковое управление ресурсами);
- Porous Defenses (Сепарированная защита)

Technical Impacts of Software Weaknesses & Detection Methods:

- Read data
- Modify data
- Denial-of-Service: unreliable execution
- Denial-of-Service: resource consumption
- Execute unauthorized code or commands
- Gain privileges / assume identity
- Bypass protection mechanism
- Hide activities

ТРИ КАТЕГОРИИ «СЛАБЫХ МЕСТ» CWE/SANS TOP 25 (CATEGORY-BASED VIEW OF THE TOP 25)

1. Insecure Interaction Between Components (Небезопасное взаимодействие между компонентами).

Примеры:

CWE-20: Improper Input Validation

CWE-116: Improper Encoding or Escaping of Output

CWE-89: Failure to Preserve SQL Query Structure (aka 'SQL Injection')

CWE-79: Failure to Preserve Web Page Structure (aka 'Cross-site Scripting')

CWE-78: Failure to Preserve OS Command Structure (aka 'OS Command Injection')

CWE-319: Cleartext Transmission of Sensitive Information

CWE-352: Cross-Site Request Forgery (CSRF)

CWE-362: Race Condition

CWE-209: Error Message Information Leak

ТРИ КАТЕГОРИИ «СЛАБЫХ МЕСТ» CWE/SANS TOP 25 (CATEGORY-BASED VIEW OF THE TOP 25)

2. Рисковое управление ресурсами подразумевает следующие слабые места ПО:

Примеры:

CWE-119: Failure to Constrain Operations within the Bounds of a Memory Buffer

CWE-642: External Control of Critical State Data

CWE-73: External Control of File Name or Path

CWE-426: Untrusted Search Path

CWE-94: Failure to Control Generation of Code (aka 'Code Injection')

CWE-494: Download of Code Without Integrity Check

CWE-404: Improper Resource Shutdown or Release

CWE-665: Improper Initialization

CWE-682: Incorrect Calculation

ТРИ КАТЕГОРИИ «СЛАБЫХ МЕСТ» CWE/SANS TOP 25 (CATEGORY-BASED VIEW OF THE TOP 25)

3. К сепарированной защите относятся:

Примеры:

CWE-285: Improper Access Control (Authorization)

CWE-327: Use of a Broken or Risky Cryptographic Algorithm

CWE-259: Hard-Coded Password

CWE-732: Insecure Permission Assignment for Critical Resource

CWE-330: Use of Insufficiently Random Values

CWE-250: Execution with Unnecessary Privileges

CWE-602: Client-Side Enforcement of Server-Side Security

CWSS: Common Weakness Scoring System

Количественные измерения: CWSS provides a quantitative measurement of the unfixed weaknesses that are present within a software application.

Общий фреймворк: CWSS provides a common framework for prioritizing security errors ("weaknesses") that are discovered in software applications.

Бизнес-приоретизация: in conjunction with the Common Weakness Risk Analysis Framework (CWRAF), CWSS can be used by consumers to identify the most important types of weaknesses for their business domains, in order to inform their acquisition and protection activities as one part of the larger process of achieving software assurance.

CWSS: СТРУКТУРА

ТРИ ГРУППЫ МЕТРИК:

Каждая группа содержит несколько метрик- так же обозначаемых как факторы (*factors*) - которые применяются для вычисления оценки CWSS score (CWSS score, between 0 and 100) для каждого слабого места.

- **Base Finding metric group (Базовые):** captures the inherent risk of the weakness, confidence in the accuracy of the finding, and strength of controls.
- **Attack Surface metric group (Поверхность атаки):** the barriers that an attacker must overcome in order to exploit the weakness.
- **Environmental metric group (Контекстные):** characteristics of the weakness that are specific to a particular environment or operational context.

CWSS: СТРУКТУРА

Base Finding

Technical Impact

Acquired Privilege

Acquired Privilege Layer

Internal Control Effectiveness

Finding Confidence

Attack Surface

Required Privilege

Required Privilege Layer

Access Vector

Authentication Strength

Level of Interaction

Deployment Scope

Environmental

Business Impact

Likelihood of Discovery

Likelihood of Exploit

External Control Effectiveness

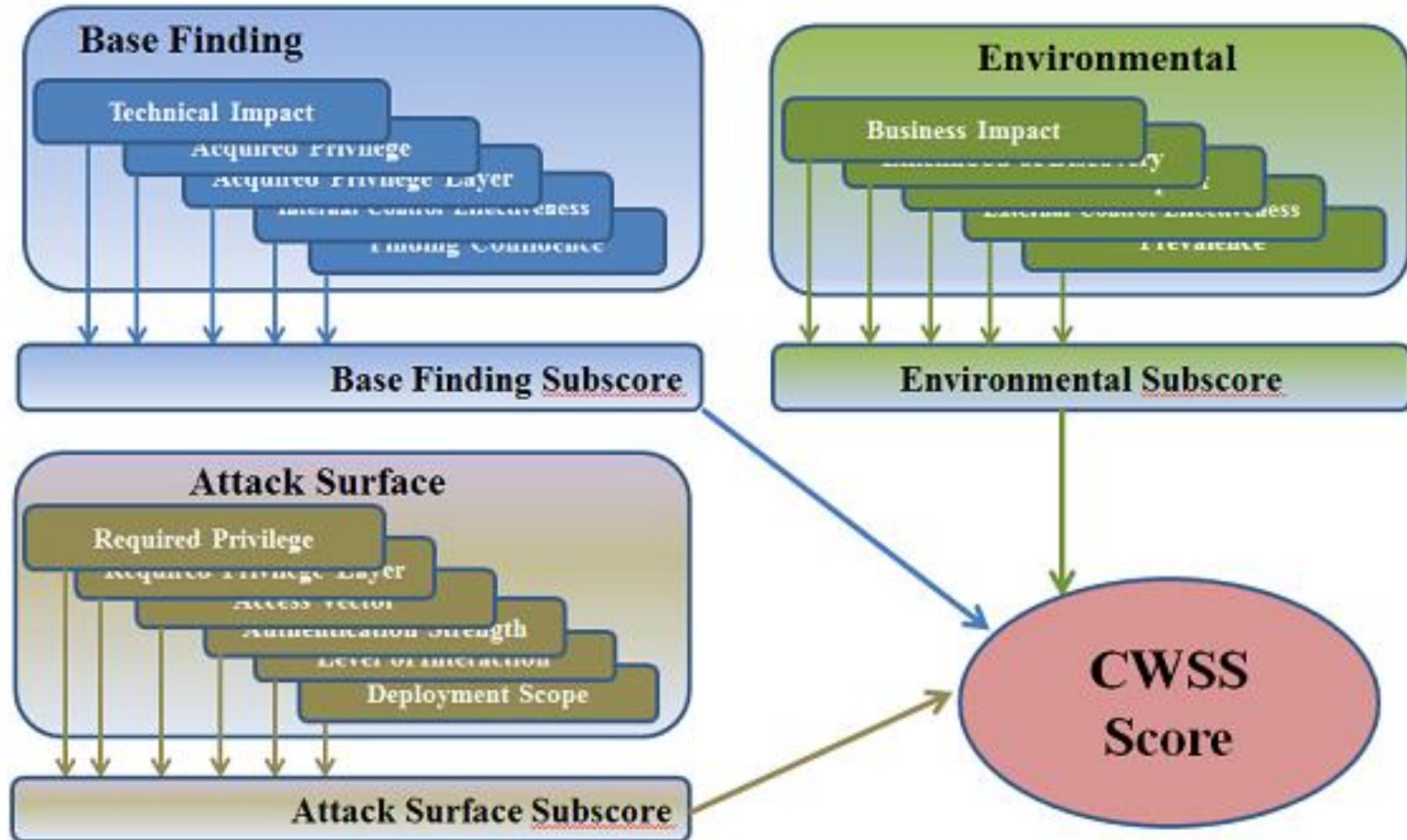
Prevalence

Группа показателей базовых: охватывает внутренние риски, присущие слабому месту, доверие к точности результатов поиска, а также действенность средств контроля.

Группа показателей области атаки: барьеры, которые должен преодолеть злоумышленник, для того чтобы эксплуатировать слабое место.

Группа показателей среды: характеристики слабого места, присущие конкретной среде или операционному контексту.

CWSS: ВЗАИМОСВЯЗЬ МЕТРИК





Оценка CWSS

Метод целевой оценки

Оцениваются отдельные слабые стороны, которые обнаруживаются при проектировании или реализации конкретного ("целевого") пакета программного обеспечения, например переполнение буфера имени пользователя в программе аутентификации в строке 1234 server.c пакета сервера FTP. Автоматизированные инструменты и консультанты по безопасности программного обеспечения используют целевые методы при оценке безопасности пакета программного обеспечения с точки зрения содержащихся в нем слабых мест.

Оценка CWSS

Метод обобщенной оценки

Оцениваются классы слабых мест, не зависящие от какого-либо конкретного пакета программного обеспечения, в целях установления их взаимных приоритетов (например, "переполнения буфера имеют более высокий приоритет, чем утечки памяти").

Данный подход используется в списках Топ- 25 CWE SANS, Топ-10 OWASP и в аналогичных исследованиях, а также в некоторых автоматических сканерах кодов. Обобщенные оценки могут существенно отличаться от целевых оценок, получаемых в результате полного анализа отдельных экземпляров класса слабых мест в конкретном пакете программного обеспечения. Например, класс переполнений буфера по-прежнему является весьма важным для многих разработчиков, но при этом отдельные ошибки переполнения буфера могут считаться менее важными, если они не могут быть непосредственно задействованы злоумышленником, и их воздействие уменьшено благодаря защитным механизмам на уровне операционной системы (ОС), таким как рандомизация распределения адресного пространства (ASLR).

Метод контекстно-адаптированной оценки

Оценки изменяются в соответствии с требованиями конкретного аналитического контекста, который может объединять приоритеты деятельности/миссии, угрозы среды, допустимый риск и т. д. Сбор этих требований осуществляется с использованием этикеток, которые увязывают присущие слабым местам характеристики с аспектами деятельности более высокого уровня. Данный метод может применяться и к целевой, и к обобщенной оценке.

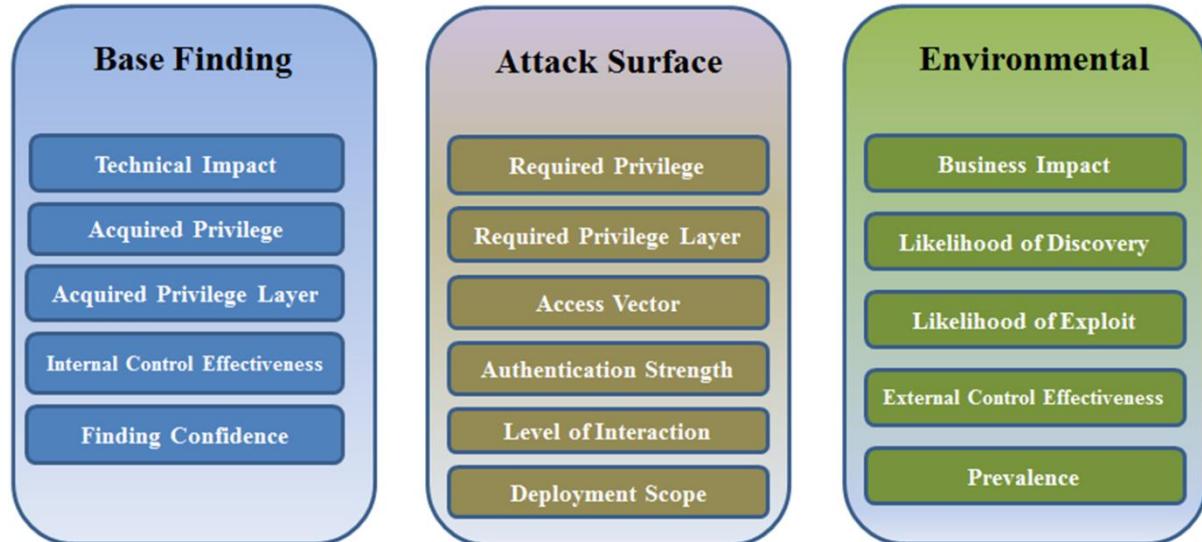
Метод агрегированной оценки

Объединяются результаты нескольких оценок слабых сторон более низкого уровня и получается единая общая оценка (или "ранг"). Применение агрегирования, возможно, наиболее уместно в целевом методе, но при этом оно может использоваться и при обобщенной оценке, как в списке Топ-25 CWE SANS.

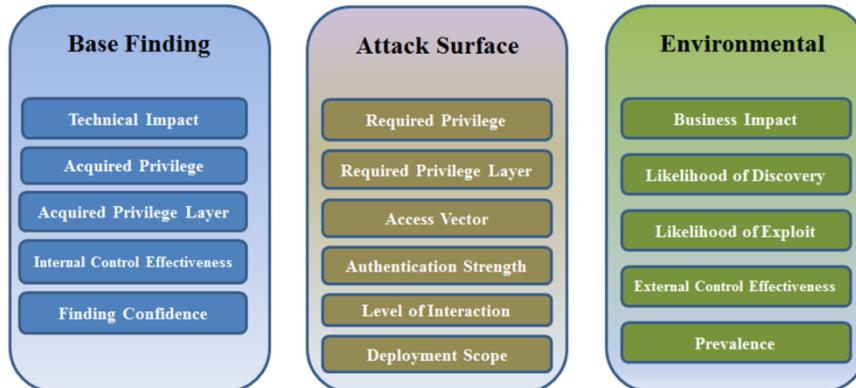
CWSS: ГРУППЫ МЕТРИК

Group	Name	Summary
Base Finding	Technical Impact (TI)	The potential result that can be produced by the weakness, assuming that the weakness can be successfully reached and exploited.
Base Finding	Acquired Privilege (AP)	The type of privileges that are obtained by an attacker who can successfully exploit the weakness.
Base Finding	Acquired Privilege Layer (AL)	The operational layer to which the attacker gains privileges by successfully exploiting the weakness.
Base Finding	Internal Control Effectiveness (IC)	the ability of the control to render the weakness unable to be exploited by an attacker.
Base Finding	Finding Confidence (FC)	the confidence that the reported issue is a weakness that can be utilized by an attacker
Attack Surface	Required Privilege (RP)	The type of privileges that an attacker must already have in order to reach the code/functionality that contains the weakness.
Attack Surface	Required Privilege Layer (RL)	The operational layer to which the attacker must have privileges in order to attempt to attack the weakness.
Attack Surface	Access Vector (AV)	The channel through which an attacker must communicate to reach the code or functionality that contains the weakness.
Attack Surface	Authentication Strength (AS)	The strength of the authentication routine that protects the code/functionality that contains the weakness.
Attack Surface	Level of Interaction (IN)	the actions that are required by the human victim(s) to enable a successful attack to take place.

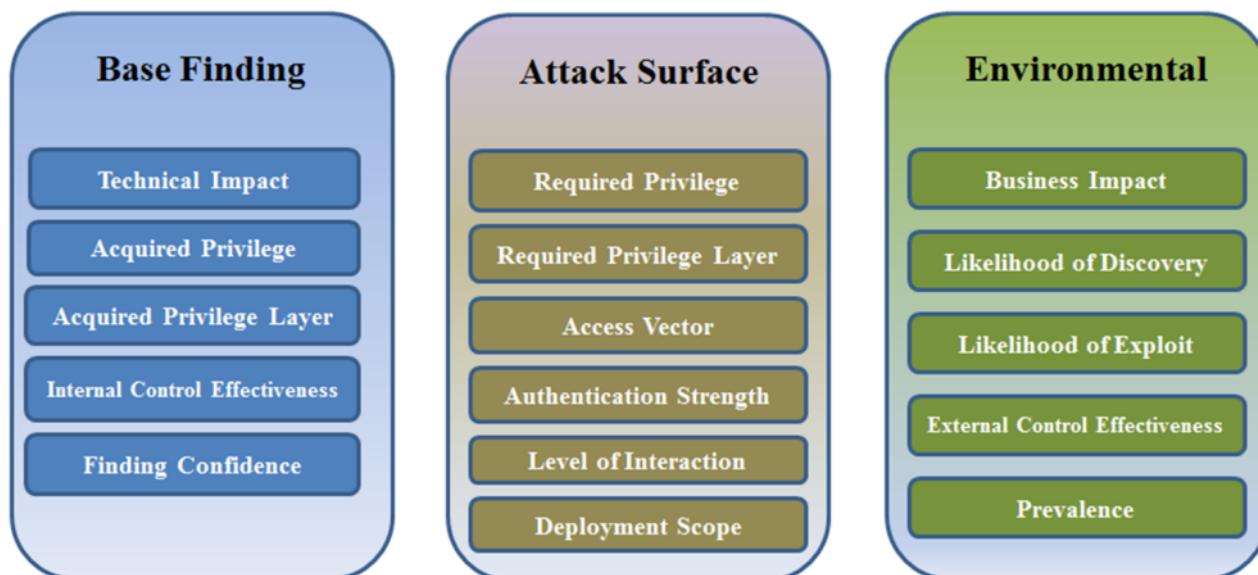
Группа	Название	Резюме
Базовые	Техническое воздействие (TI)	Потенциальный результат, к которому может привести слабое место, при условии, что к этому слабому месту можно успешно получить доступ, и оно может успешно эксплуатироваться
	Приобретенная привилегия (AP)	Тип привилегий, получаемых злоумышленником, который может успешно эксплуатировать слабое место
	Уровень приобретенной привилегии (AL)	Операционный уровень, для которого злоумышленник получает привилегии за счет успешной эксплуатации слабого места
	Эффективность внутреннего контроля (IC)	Способность средств контроля сделать слабое место непригодным для эксплуатации злоумышленником
	Доверие к результатам поиска (FC)	Уверенность в том, что обнаруженная проблема является слабым местом, которое может быть использовано злоумышленником



Группа	Название	Резюме
Поверхность атаки	Требуемая привилегия (RP)	Тип привилегий, которые уже должен иметь злоумышленник, для того чтобы получить доступ к коду/функциональной возможности, содержащим слабое место
	Уровень требуемой привилегии (RL)	Операционный уровень, для которого злоумышленник должен иметь привилегии, чтобы попытаться атаковать слабое место
	Вектор доступа (AV)	Канал, по которому злоумышленник должен обмениваться информацией, чтобы получить доступ к коду или функциональной возможности, содержащим слабое место
	Сложность аутентификации (AS)	Сложность программы аутентификации, которая обеспечивает защиту кода/функциональной возможности, содержащих слабое место
	Уровень взаимодействия (IN)	Действия, которые должно совершить лицо(а), являющееся объектом атаки, чтобы создать условия для ее успешного осуществления
	Масштаб развертывания (DS)	Присутствие слабого места либо во всех развертываемых экземплярах программного обеспечения, либо ограниченно в ряде платформ и/или конфигураций



Группа	Название	Резюме
Среда	Воздействие на деятельность (BI)	Потенциальное воздействие на деятельность или миссию в случае успешной эксплуатации слабого места
	Вероятность обнаружения (DI)	Вероятность того, что злоумышленник может обнаружить слабое место
	Вероятность эксплуатации (EX)	Вероятность того, что, в случае обнаружения слабого места, злоумышленник, обладающий требуемыми привилегиями/аутентификацией/доступом, сможет его успешно эксплуатировать
	Эффективность внешнего контроля (EC)	Возможность контроля или смягчения последствий, не относящаяся к программному обеспечению, которая может затруднить доступ злоумышленника к слабому месту и его задействование злоумышленником
	Распространенность (P)	Частота появления слабого места данного типа в программном обеспечении



Base Finding group

Группа базовых показателей



Base Finding

Technical Impact

Acquired Privilege

Acquired Privilege Layer

Internal Control Effectiveness

Finding Confidence

Attack Surface

Required Privilege

Required Privilege Layer

Access Vector

Authentication Strength

Level of Interaction

Deployment Scope

Environmental

Business Impact

Likelihood of Discovery

Likelihood of Exploit

External Control Effectiveness

Prevalence

Technical Impact

Техническое воздействие (TI)

Значение	Код	Вес	Описание
Критическое Critical	C	1,0	Полный контроль анализируемого программного обеспечения до такого уровня, когда невозможно осуществлять операции
Высокое High	H	0,9	Существенный контроль анализируемого программного обеспечения или возможность получения доступа к важнейшей информации
Среднее Medium	M	0,6	Умеренный контроль анализируемого программного обеспечения или возможность получения доступа к информации средней важности
Низкое Low	L	0,3	Минимальный контроль анализируемого программного обеспечения или возможность получения доступа только к относительно маловажной информации
Отсутствует None	N	0,0	Полное отсутствие технического воздействия на анализируемое программное обеспечение. Иными словами, это не приведет к уязвимости
По умолчанию Default	D	0,6	Весовой коэффициент для стандартного значения – это медиана весовых коэффициентов для значений "Критическое", "Высокое", "Среднее", "Низкое" и "Отсутствует"
Неизвестно Unknown	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Данный параметр может не применяться в среде с высокими требованиями к гарантии; пользователь, возможно, хочет изучить каждый интересующий результат поиска слабых мест, независимо от уровня доверия
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов

Acquired privilege

Приобретенная привилегия (AP)

Приобретенная привилегия определяет тип привилегий, получаемых злоумышленником, который может успешно эксплуатировать слабое место.

*В некоторых случаях значение параметра "приобретенная привилегия" может быть таким же, как у параметра "требуемая привилегия", что предполагает либо:

- (1) "горизонтальное" расширение привилегий (например, от одного непrivилегированного пользователя другому – Lateral Movement),
- (2) расширение привилегий в рамках песочницы (Sandbox).

Acquired privilege

Приобретенная привилегия (AP) - 1

Значение	Код (прим.)	Вес	Описание
Администратор	A	1,0	Злоумышленник получает доступ к объекту с привилегиями администратора, корневого пользователя, с системными или эквивалентными им привилегиями, что предполагает полный контроль анализируемого программного обеспечения; или же злоумышленник может расширить собственные привилегии (более низкого уровня) до привилегий администратора
Частично привилегированный пользователь	P	0,9	Злоумышленник получает доступ к объекту с некоторыми особыми привилегиями, но не достаточными, чтобы соответствовать привилегиями администратора; или же злоумышленник может расширить собственные привилегии (более низкого уровня) до привилегий частично привилегированного пользователя. Например, пользователь может иметь привилегии, позволяющие делать резервные копии, но не изменять конфигурацию программного обеспечения или устанавливать обновления
Обычный пользователь	RU	0,7	Злоумышленник получает доступ к объекту, являющемуся обычным пользователем без особых привилегий; или же злоумышленник может расширить собственные привилегии (более низкого уровня) до привилегий обычного пользователя
Ограниченнaя/ гостевая	L	0,6	Злоумышленник получает доступ к объекту с ограниченными или "гостевыми" привилегиями, которые могут существенно ограничивать допустимые действия; или же злоумышленник может расширить собственные привилегии (более низкого уровня) до гостевых привилегий. Примечание: данное значение не касается понятия "гостевой операционной системы" в виртуализованных хост-компьютерах

NOTE – A mnemonic for the main values in this factor is "RUNLAP" (Regular User, None, Limited, Admin, Partially-Privileged).

Acquired privilege

Приобретенная привилегия (AP) - 2

Значение	Код (прим.)	Вес	Описание
Отсутствует	N	0,1	Злоумышленник не может получить доступ к каким бы то ни было дополнительным привилегиям, помимо тех, которые у него уже имеются. (Следует отметить, что данное значение целесообразно использовать в ограниченных случаях, когда злоумышленник может выйти из песочницы или иной среды с ограниченными возможностями, но еще не может получить дополнительные привилегии и не может получить доступ как другие пользователи)
По умолчанию	D	0,7	Медиана весовых коэффициентов для значений "Отсутствует", "Гостевой", "Обычный пользователь", "Частично привилегированный пользователь" и "Администратор"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации.
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом.
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Следует отметить, что количественные значения поддерживаются для полноты; однако в связи с тем, что привилегии и пользователи являются отдельными объектами, может существовать лишь ограниченное число случаев, в которых целесообразно использовать количественную модель

NOTE – A mnemonic for the main values in this factor is "RUNLAP" (Regular User, None, Limited, Admin, Partially-Privileged).

Acquired privilege layer (AL)

Уровень приобретенной привилегии

Значение	Код	Вес	Описание
Приложение Application	A	1,0	Злоумышленник приобретает привилегии, которые поддерживаются в самом анализируемом программном обеспечении. (Если анализируемое программное обеспечение является одной из важнейших частей базовой системы, например, ядром операционной системы, то, возможно, более целесообразно использовать значение "Система")
Система System	S	0,9	Злоумышленник приобретает привилегии для системы или физического хоста, которые используются для прогона анализируемого программного обеспечения
Сеть Network	N	0,7	Злоумышленник приобретает привилегии для доступа в сеть
Инфраструктура Infrastructure	E	1,0	Злоумышленник приобретает привилегии для одного из важнейших участков инфраструктуры предприятия, например, маршрутизатора, коммутатора, системы наименований доменов (DNS), контроллера домена, брандмауэра, сервера определения идентичности и т. д.
По умолчанию	D	0,9	Медиана весовых коэффициентов для значений "Приложение", "Система", "Сеть" и "Инфраструктура предприятия"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации.
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом.
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Следует отметить, что количественные значения поддерживаются для полноты; однако в связи с тем, что уровни привилегии являются отдельными объектами, может существовать лишь ограниченное число случаев, в которых целесообразно использовать количественную модель

NOTE – A mnemonic for the main values in this factor is "SANE" (System, Application, Network, Enterprise Infrastructure).

Internal control effectiveness (IC)

Эффективность внутренних контролей

Внутренний контроль – это средство контроля, механизм защиты или иной способ уменьшения влияния, который в явном виде встроен в программное обеспечение (через архитектуру, проектирование или реализацию).

Эффективность внутреннего контроля измеряет способность средств контроля сделать слабое место непригодным для эксплуатации злоумышленником. Например, программа проверки вводимых значений, ограничивающая длину вводимого значения 15 символами, может быть сравнительно эффективна в отношении межсайтовых атак с внедрением сценария (XSS) благодаря уменьшению размера эксплойта XSS, который могут попытаться проэксплуатировать.

Internal control effectiveness (IC)

Эффективность внутренних контролей

Значение	Код	Вес	Описание
Отсутствует	N	1,0	Средства контроля отсутствуют
Ограниченный Limited	L	0,9	Имеются упрощенные методы или случайные ограничения, которые могут не позволить недостаточно подготовленному злоумышленнику эксплуатировать эту ошибку
Умеренный Moderate	M	0,7	Механизм защиты широко используется, но имеет известные ограничения, которые опытный нарушитель может обойти, приняв некоторые меры. Например, использование кодирования объектов в языке описания гипертекстовых документов (HTML) для предотвращения атак XSS можно обойти, если поместить выходные данные в другой контекст, например, в атрибут метки в каскадной таблице стилей (CSS) или HTML
Косвенный (эшелонированная защита) Indirect (Defense-in-depth)	I	0,5	Средства контроля не обеспечивают реальной защиты от эксплуатации слабого места, но косвенным образом уменьшают воздействие, в случае если предпринята успешная атака, или иным образом затрудняют создание работоспособного эксплойта. Например, программа проверки может косвенным образом ограничивать размер вводимого значения, что может затруднить создание злоумышленником вредоносной нагрузки для атаки XSS или атаки с внедрением кода языка структурированных запросов (SQL)
Наилучший имеющийся Best-available	B	0,3	Контроль соответствует существующему передовому опыту, но ему могут быть присущи некоторые ограничения, позволяющие опытному злоумышленнику, имеющему четкую цель, преодолеть контроль, при этом может требоваться наличие других слабых мест. Например, метод двойного представления для защиты от подделки межсайтовых запросов (CSRF) считается одним из самых действенных среди имеющихся, но его можно обойти, использовав одновременно поведение определенных функциональных возможностей, которые могут считывать необработанные заголовки HTTP
Полный Complete	C	0,0	Средство контроля абсолютно эффективно противодействует слабому месту, то есть отсутствуют ошибка и уязвимость, а также отрицательные последствия эксплуатации этой проблемы. Например, операция копирования в буфер, при которой всегда обеспечивается превышение размера буфера получателя над размером источника (вместе с любым косвенным увеличением первоначального размера источника), не вызовет переполнения буфера

Finding confidence (FC)

Доверие к результатам поиска

Доверие к результатам поиска – это уверенность в том, что обнаруженная проблема:

- 1) является слабым местом;
- 2) может быть задействована или использована злоумышленником.

Значение	Код	Вес	Описание
Подтверждено	T	1,0	Злоумышленник может получить доступ к слабому месту
Локально подтверждено	LT	0,8	Слабое место возникает в отдельной функции или компоненте, в дизайне которого используется безопасный вызов данной функции, однако возможность доступа злоумышленника к данной функции неизвестна или отсутствует. Например, служебная функция может создавать запрос к базе данных, не кодируя его вводимые значения, однако если она вызывается только с помощью строковых констант, то результат поиска является локально подтвержденным
Не подтверждено	F	0,0	Результат поиска является ошибочным (то есть результат не подтвержден и слабое место отсутствует) и/или отсутствует возможная роль злоумышленника
Стандартное значение	D	0,8	Медиана весовых коэффициентов для значений "Подтверждено", "Локально подтверждено" и "Не подтверждено"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации.
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Данный параметр может не применяться в среде с высокими требованиями к гарантии; пользователь, возможно, хочет изучить каждый интересующий результат поиска слабых мест, независимо от уровня доверия
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Некоторые инструменты анализа кода включают точные измерения точности конкретных схем обнаружения

Attack Surface metric group

Группа метрик Поверхности Атаки



Base Finding

Technical Impact

Acquired Privilege

Acquired Privilege Layer

Internal Control Effectiveness

Finding Confidence

Attack Surface

Required Privilege

Required Privilege Layer

Access Vector

Authentication Strength

Level of Interaction

Deployment Scope

Environmental

Business Impact

Likelihood of Discovery

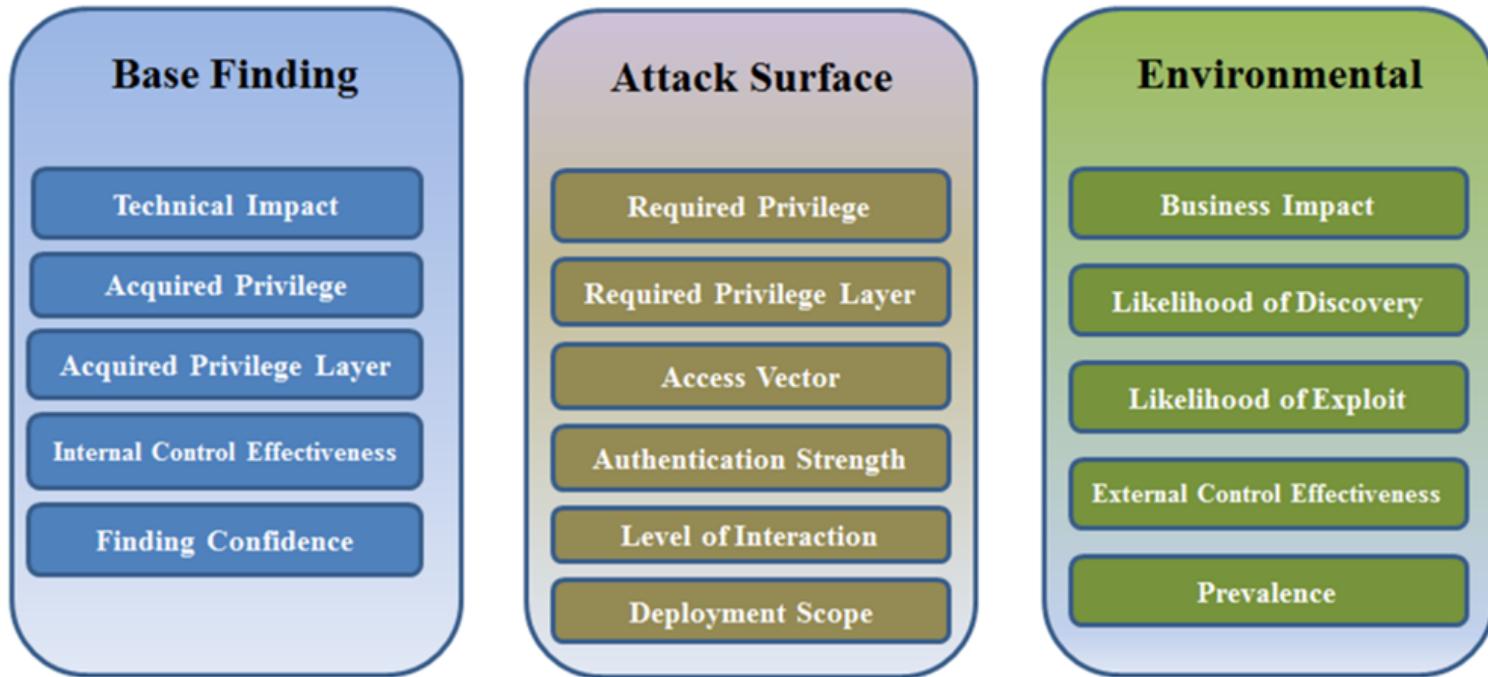
Likelihood of Exploit

External Control Effectiveness

Prevalence

Attack Surface metric group

Группа метрик Поверхности Атаки



Метрическая группа поверхности атаки состоит из следующих факторов:

- Требуемые привилегии - Required privilege (RP)
- Требуемый уровень привилегий (слой) - Required privilege layer (RL)
- Вектор доступа - Access vector (AV)
- Уровень аутентификации - Authentication strength (AS)
- Уровень взаимодействия - Level of interaction (IN)
- Область развертывания - Deployment scope (SC)

Требуемые привилегии

Required privilege (RP)

Значение	Код	Вес	Описание
Нет	N	1.0	Никаких привилегий не требуется. Например, веб-поисковая система может не требовать каких-либо привилегий для объекта для ввода поискового запроса и просмотра результатов.
Ограниченный/Гость	L	0.9	Субъект имеет ограниченные или "гостевые" привилегии, которые могут значительно ограничить разрешенные действия; субъект может быть в состоянии зарегистрировать или создать новую учетную запись без каких-либо специальных требований или подтверждения личности. Например, веб-блог может позволить участникам создать имя пользователя и отправить действительный адрес электронной почты перед вводом комментариев. Примечание: это значение не относится к понятию "гостевая операционная система" в хостах.
Обычный пользователь	RU	0.7	Это обычный пользователь, не имеющий особых привилегий
Частично привилегированный пользователь	P	0.6	Субъект является пользователем с некоторыми особыми привилегиями, но не такими как у администратора. Например, пользователь может иметь привилегии для создания резервных копий, но не для изменения конфигурации программного обеспечения или установки обновлений.
Администратор	A	0.1	Субъект имеет права администратора, администратора системы или пользователя, который имеет полный контроль над программным обеспечением или базовой ОС.
По умолчанию	D	0.7	Права обычного пользователя, которые похожи на частично привилегированного пользователя и администратора.
Неизвестный	UK	0.5	Информации о данном пользователе не найдено. В дальнейшем возможно изменение, которое может повлиять на изменение оценки.
NOTE – A mnemonic for the main values in this factor is "RUNLAP" (Regular User, None, Limited, Admin, Partially-Privileged).			

Требуемый слой привилегии

Required privilege layer (RL)

Значение	Код	Вес	Описание
Приложение	A	1.0	Злоумышленник должен иметь привилегии, которые поддерживаются в самом анализируемом программном обеспечении. (Если анализируемое программное обеспечение является существенной частью базовой системы, такой как ядро операционной системы, то системное значение может быть более подходящим.)
Система	S	0.9	Злоумышленник должен иметь права доступа к базовой системе или физическому хосту, используемому для запуска анализируемого программного обеспечения.
Сеть	N	0.7	Злоумышленник должен иметь права доступа к сети.
Инфраструктура	E	1.0	Злоумышленник должен иметь права доступа к критически важным элементам корпоративной инфраструктуры, таким как маршрутизатор, коммутатор, DNS, контроллер домена, брандмауэр, сервер идентификации и т. д.
По умолчанию	D	0.9	Защита для прикладной, системной, сетевой и корпоративной инфраструктуры.
Неизвестный	UK	0.5	Информации о данном пользователе не найдено. В дальнейшем возможно изменение, которое может повлиять на изменение оценки.
Не определено	NA	1.0	Этот фактор может быть неприменим в среде с высокими требованиями к обеспечению безопасности, которая требует строгого соблюдения разделения привилегий даже между уже привилегированными пользователями.
Количественное значение	Q		Этот фактор может быть количественно определен. Обратите внимание, что количественные значения поддерживаются для полноты; однако, поскольку привилегии и пользователи являются дискретными сущностями, могут существовать ограниченные обстоятельства, в которых количественная модель была бы полезна.

NOTE – A mnemonic for the main values in this factor is "SANE" (System, Application, Network, Enterprise Infrastructure).

Вектор доступа Access vector (AV)

Вектор доступа определяет канал, по которому злоумышленник должен обмениваться информацией, чтобы получить доступ к коду или функциональной возможности, содержащими слабое место.

! Следует отметить, что эти значения весьма схожи со значениями, используемыми в CVSS, за исключением того, что в CWSS проводится различие между физическим доступом и местным (оболочка/учетная запись) доступом.

Притом что между вектором доступа и уровнем требуемой привилегии существует тесная взаимосвязь, эти два параметра различны.

!! Например, злоумышленник, имеющий "физический" доступ к маршрутизатору, может обладать способностью затронуть сеть или уровень предприятия.

Вектор доступа Access vector (AV)

Значение	Код	Вес	Описание
Интернет	I	1.0	Злоумышленник должен иметь доступ к Интернету, чтобы добраться до слабого места.
Интеранет	R	0.8	Злоумышленник должен иметь доступ к внутренней сети предприятия, которая защищена от прямого доступа из интернета, например с помощью брандмауэра, при этом без использования интернета внутренняя сеть доступна для большинства сотрудников предприятия.
Частная сеть	V	0.8	Злоумышленник должен иметь доступ к частной сети, которая доступна узко определенному кругу доверенных сторон.
Соседняя сеть	A	0.7	Злоумышленник должен иметь доступ к физическому интерфейсу с сетью, например домену широковещательной передачи или домену коллизий, относящимся к уязвимому программному обеспечению. К примерам локальных сетей относятся локальная подсеть на базе протокола Интернет (IP), Bluetooth, IEEE 802.11 и локальный сегмент Ethernet.
Локальный	L	0.5	Злоумышленник должен иметь интерактивную локальную (оболочка) учетную запись, которая имеет прямой интерфейс с базовой операционной системой.
Физический	P	0.2	Злоумышленник должен иметь физический доступ к системе, в которой работает программное обеспечение, или, в противном случае, он должен иметь возможность взаимодействия с системой через такие интерфейсы, как универсальная последовательная шина (USB), компакт-диск (CD), клавиатура, мышь и т. д.
По умолчанию	D	0.75	Медиана весовых коэффициентов для соответствующих значений.
Неизвестный	U	0.5	
Не применяется	NA	1.0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом.
Количественное	Q		Этот фактор может быть количественно определен.

Сложность аутентификации Authentication strength (AS)

Сложность аутентификации охватывает сложность программы аутентификации, которая обеспечивает защиту кода/функциональной возможности, содержащих слабое место.

Если используется несколько программ аутентификации или если существует две и более ветвей кода, оценка должна выполняться следующим образом:

В случае нескольких программ аутентификации или нескольких ветвей кода, по которым можно достичь того же слабого места, применяется следующий руководящий принцип.

- Для каждой ветви кода проводится анализ каждой программы аутентификации, существующей на данной ветви кода, и выбирается значение с наименьшим весовым коэффициентом (то есть программа самой строгой аутентификации на данной ветви кода). Это значением называется значением ветви кода.
- Осуществляется сбор всех значений ветви кода.
- Выбирается значение ветви кода, имеющее наибольший весовой коэффициент (то есть имеющее самую слабую программу).

В данном методе каждая ветвь кода оценивается по самой строгой программе аутентификации данной ветви (поскольку злоумышленнику потребуется обойти данное средство контроля), затем выбирается наименее защищенная ветвь кода (то есть самый легкий путь, по которому пойдет злоумышленник).

Сложность аутентификации Authentication strength (AS)

Значение	Код	Вес	Описание
Строгая	S	0.7	Слабое место обуславливает потребность в наиболее строгом из имеющихся методов для привязки данного объекта к реальной идентичности, например таком, как аппаратные жетон и/или многофакторная аутентификация.
Средняя	M	0.8	Слабое место обуславливает потребность в аутентификации с использованием умеренно строгих методов, таких как применение сертификатов от недоверенных органов, аутентификации на основе знаний или одноразовых паролей.
Слабая	W	0.9	Слабое место обуславливает потребность в методе простой, слабой аутентификации, который легко вскрывается с помощью спуфинга, словаря или атак с повтором, таких как неизменный пароль.
Отсутствует	N	1.0	Не требует никакой аутентификации вообще.
По умолчанию	D	0.85	Медиана весовых коэффициентов для значений "Строгая", "Средняя", "Слабая" и "Отсутствует".
Неизвестно	UK	0.5	Информации для определения значения этого фактора недостаточно.
Не применяется	NA	1.0	Этот фактор может быть неприменим в среде с высокими требованиями к обеспечению безопасности, которая требует строгого соблюдения разделения привилегий даже между уже привилегированными пользователями.
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов

Уровень взаимодействия

Level of interaction (IN)

Уровень взаимодействия охватывает действия, которые необходимо совершить лицу/лицам, являющемуся/являющимся объектом атаки, для того чтобы создать условия для ее успешного осуществления.

Значение	Код	Вес	Описание
Автоматическое	A	1.0	Взаимодействия с человеком не требуется.
Типовое/ ограниченное	T	0.9	Злоумышленник должен убедить пользователя выполнить действие, которое является общим или рассматривается как "обычное" в рамках типового режима работы продукта. Например, щелчок по ссылке на веб-страницу или предварительный просмотр тела письма, пришедшего по электронной почте, являются общим поведением.
Среднее	M	0.8	Злоумышленник должен убедить пользователя выполнить действие, которое осмотрительному знающему пользователю может показаться подозрительным. Например, пользователь должен принять предупреждение, в котором предполагается, что полезная нагрузка злоумышленника может содержать опасный контент.
Уступающее (Opportunistic)	O	0.3	Злоумышленник не может напрямую контролировать объект атаки или воздействовать на него, а может лишь пассивно извлекать выгоду из ошибок и действий других.
Высокое	H	0.1	Требуется весьма обширная психологическая атака, возможно включающая использование неосведомленности объекта атаки или неосторожности с его стороны.
Без взаимодействия	NI	0.0	Не существует возможного взаимодействия, даже уступающего вместо того, чтобы вести к уязвимости, это будет, как правило, представлять слабое место как "ошибку". С учетом того что CWSS служит для безопасности, весовой коэффициент составляет 0.
По умолчанию	D	0.55	Медиана для значений "Автоматическое", "Ограниченнное", "Среднее", "Уступающее", "Высокое" и "Взаимодействие отсутствует".
Неизвестно	UK	0.5	Информации для определения значения этого фактора недостаточно.

Масштаб развертывания

Deployment scope (SC)

Масштаб развертывания определяет, присутствует ли слабое место во всех развертываемых экземплярах программного обеспечения или оно ограничено поднабором платформ и/или конфигураций. Например, ошибка числового решения может применяться только к программному обеспечению, которое запускается в среде определенной ОС и в 64-битовой архитектуре, а проблема обхода каталога может затрагивать только операционные системы, в которых символ "\" интерпретируется как разделитель каталогов.

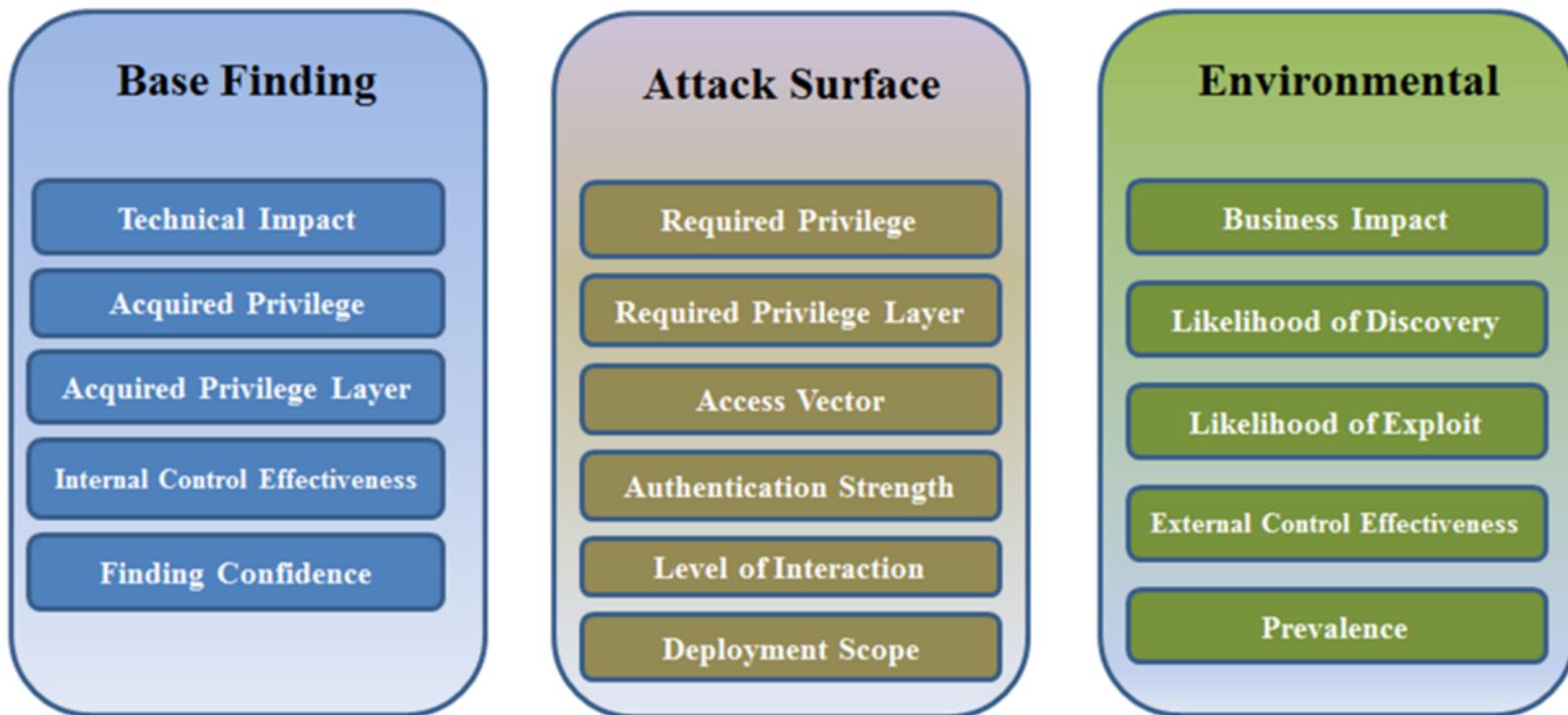
Значение	Код	Вес	Описание
Полное (All)	A	1.0	Присутствует во всех платформах или конфигурациях.
Среднее (Moderate)	M	0.9	Присутствует в общих платформах или конфигурациях.
Встречается редко (Rare)	R	0.5	Только в редких платформах и конфигурациях.
Потенциально достижимое (Potentially Reachable)	P	0.1	Потенциально достижимое *, однако все ветви кода на текущий момент являются безопасными и/или слабое место находится в недоступном участке программы.
По умолчанию	D	0.7	Медиана весовых коэффициентов.
Неизвестно	UK	0.5	Информации для определения значения этого фактора недостаточно.
Не применяется	NA	1.0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом.
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Пользователь может знать, какая процентная доля отправленного (или поддерживаемого) программного обеспечения содержит эту ошибку.

NOTE 1 – A mnemonic for the main values in this factor is "RAMP" (Rare, All, Moderate, Potentially Reachable).

NOTE 2 – "Potentially Reachable" has some overlap with "Locally True" in the Finding Confidence (FC) factor.

Environmental Metric group

Группа показателей среды



Группа показателей среды состоит из следующих параметров:

- воздействие на деятельность (BI);
- вероятность обнаружения (DI);
- вероятность эксплуатации (EX);
- эффективность внешнего контроля (EC);
- распространенность (P).

Воздействие на деятельность Business Impact (BI)

Воздействие на деятельность описывает потенциальное воздействие на деятельность или миссию в случае успешной эксплуатации слабого места.

ПРИМЕЧАНИЕ. Поскольку связанные с деятельностью вопросы в значительной степени зависят от конкретной организации, в CWSS не предпринимается попытки провести более детальную разбивку, например по показателю финансового, репутационного, физического, юридического или иного ущерба. Этот параметр может оцениваться количественно для поддержки моделей, определенных внешне.

Значение	Код	Вес	Описание
Критическое	C	1.0	Деятельность/миссия может оказаться невыполнимой.
Высокое	H	0.9	Операции в рамках деятельности/миссии будут существенным образом затронуты.
Среднее	M	0.6	Бизнес /задание будут затронуты, но без значительного ущерба для регулярных операций.
Низкое	L	0.3	Минимальное влияние на бизнес.
Отсутствует	N	0.0	Воздействие отсутствует.
Стандартное значение	D	0.6	Медиана весовых коэффициентов для значений "Критическое", "Высокое", "Среднее", "Низкое" и "Отсутствует".
Неизвестно	UK	0.5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку.
Не применяется	NA	1.0	<p>Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом.</p> <p>Данный параметр может не применяться в тех условиях, когда неактуален показатель воздействия на деятельность или когда воздействие оценивается и рассматривается в аналитических процессах, не входящих в саму оценку CWSS.</p>
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. В некоторых организациях могут применяться специальные измерения бизнес-ценности актива, например такие, которые могут быть интегрированы в данное измерение.

Вероятность обнаружения

Likelihood of Discovery(DI)

Вероятность обнаружения – это вероятность того, что злоумышленник может обнаружить слабое место.

ПРИМЕЧАНИЕ. Рассматривался вопрос об исключении этого параметра из CWSS 1.0, поскольку могут возникнуть трудности при его измерении и на него могут оказывать воздействие другие параметры, такие как "Приобретенная привилегия", "Техническое воздействие" и "Распространенность". Однако он был сохранен для отражения того факта, что некоторые разработчики будут использовать параметр "Вероятность обнаружения" при определении срочности разрешения какой-либо проблемы.

Значение	Код	Вес	Описание
Высокая	H	1.0	С высокой вероятностью злоумышленник сможет обнаружить слабое место быстро и с малыми усилиями, используя простые методы, без доступа к исходному коду или иным артефактам, упрощающим обнаружение слабого места.
Средняя	M	0.6	Злоумышленник может выявить слабое место, но для этого потребуются определенные навыки, возможно доступ к исходному коду или реверсивное воспроизведение. Обнаружение проблемы может потребовать определенных затрат времени.
Низкая	L	0.2	Маловероятно, что злоумышленник сможет обнаружить слабое место, не имея узкоспециальных навыков, доступа к исходному коду (или его эквиваленту) и без существенных затрат времени.
Стандартное значение	D	0.6	Медиана для значений "Высокая", "Средняя" и "Низкая".
Неизвестно	UK	0.5	Информации для определения значения этого фактора недостаточно. Возможно, потребуется дальнейший анализ. В будущем может быть выбрано другое значение, которое может повлиять на оценку.
Не применяется	NA	1.0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Этот параметр может не применяться, если эксперт предполагает, что злоумышленник обнаружит все слабые места.
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов.

Вероятность эксплуатации

Likelihood of exploit (EX)

Вероятность эксплуатации – это вероятность того, что, в случае обнаружения слабого места, злоумышленник, обладающий требуемыми привилегиями/аутентификацией/доступом, сможет его успешно эксплуатировать.

! Следует отметить, что на данный параметр влияет показатель воздействия слабого места, так как злоумышленники зачастую нацеливаются на слабые места, вызывающие наиболее серьезные последствия. В качестве альтернативы они могут нацеливаться на слабые места, которые легко задействовать (CWE Chain).

Цепочка (CWE Chain) - сложный элемент, представляющий собой последовательность двух или более отдельных слабых мест, которые могут быть тесно связаны между собой в рамках программного обеспечения. Одна слабость, X, может непосредственно создать условия, необходимые для того, чтобы другая слабость, Y, вошла в уязвимое состояние. Когда это происходит, CWE обращается к X как к "первичному" Y, а Y является "результирующим" от X. Цепочки могут включать более двух слабых мест, и в некоторых случаях они могут иметь древовидную структуру.

For example, if an integer overflow (CWE-190) occurs when calculating the amount of memory to allocate, an undersized buffer will be created, which can lead to a buffer overflow (CWE-120). In this case, the integer overflow would be primary to the buffer overflow. Chains can involve more than two weaknesses, and in some cases, they might have a tree-like structure.

https://cwe.mitre.org/data/reports/chains_and_composites.html

На этот параметр влияют также другие параметры, такие как эффективность внутреннего и внешнего контроля. Может представляться, что влияние также оказывает распространенность, однако распространенность более тесно связана с вероятностью обнаружения.

Вероятность эксплуатации

Likelihood of exploit (EX)

Значение	Код	Вес	Описание
Высокая	H	1.0	С высокой вероятностью злоумышленник успешно поразит выбранное целью данное слабое место, имея надежный экспloit, который легко можно развивать.
Средняя	M	0.6	Злоумышленник вероятно успешно поразит выбранное целью данное слабое место, однако его шансы на успех могут изменяться или же для успешного осуществления потребуется несколько попыток.
Низкая	L	0.2	Злоумышленник вероятно не поразит выбранное целью данное слабое место или имеет ограниченные шансы на успех.
Отсутствует	N	0.0	Злоумышленник не имеет шансов на успех, то есть проблема является "ошибкой", так как отсутствует участие злоумышленника и отсутствуют выгоды для злоумышленника.
Стандартное значение	D	0.6	Медиана для значений "Высокая", "Средняя" и "Низкая". Значение "Отсутствует" не учитывается, исходя из предположения, что с использованием этого значения будет оценено малое число результатов поиска слабых мест, а его включение в расчет медианы сократит весовой коэффициент до неинтуитивного уровня.
Неизвестно	UK	0.5	Для присвоения значения данному параметру недостаточно информации.
Не применяется	NA	1.0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Например, эксперт пожелает сделать допущение о том, что злоумышленники могут эксплуатировать любое слабое место, которое найдут, или готовы направить существенные ресурсы для обхода любых возможных барьеров в целях развития успеха.
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов.

Эффективность внешнего контроля

External control effectiveness (EC)

Эффективность внешнего контроля – это возможность контроля или смягчения последствий, не относящаяся к программному обеспечению, которая может затруднить доступ злоумышленника к слабому месту и его задействование злоумышленником.

Например, рандомизация распределения адресного пространства (ASLR) и аналогичные методы снижают, но не ликвидируют шансы на успех атаки "переполнение буфера". Однако ASLR не реализуется напрямую в самом программном обеспечении.

В случае нескольких средств внешнего контроля или нескольких ветвей кода, по которым можно достичь того же слабого места, применяется следующий руководящий принцип:

- Для каждой ветви кода проводится анализ каждого средства внешнего контроля, существующего на данной ветви кода, и выбирается значение с наименьшим весовым коэффициентом (то есть самое действенное средство внешнего контроля на данной ветви кода). Это значение называется значением ветви кода.
- Осуществляется сбор всех значений ветви кода.
- Выбирается значение ветви кода, имеющее наибольший весовой коэффициент (то есть наименее действенное средство контроля).

В данном методе каждая ветвь кода оценивается по самому действенному средству контроля данной ветви (поскольку злоумышленнику потребуется обойти данное средство контроля), затем выбирается наименее защищенная ветвь кода (то есть самый легкий путь, по которому пойдет злоумышленник).

Эффективность внешнего контроля

External control effectiveness (EC)

Значение	Код	Вес	Описание
Отсутствует	N	1.0	Средства контроля отсутствуют.
Ограниченный	L	0.9	Имеются упрощенные методы или случайные ограничения, которые могут не позволить недостаточно подготовленному злоумышленнику эксплуатировать эту проблему.
Умеренный	M	0.7	Механизм защиты широко используется, но имеет известные ограничения, которые опытный нарушитель может обойти, приняв некоторые меры.
Косвенный (эшелонирован- ная защита)	I	0.5	Средство контроля не обеспечивает реальной защиты от эксплуатации слабого места, но косвенным образом уменьшает воздействие, в случае если предпринята успешная атака, или иным образом затрудняют создание работоспособного эксплойта. Например, рандомизация распределения адресного пространства (ASLR) и аналогичные методы снижают, но не ликвидируют шансы на успех атаки "переполнение буфера". С учетом того что ответной реакцией является, как правило, выход из процесса, то результатом будет и отказ в обслуживании.
Наилучший имеющийся	B	0.3	Контроль соответствует существующему передовому опыту, но ему могут быть присущи некоторые ограничения, позволяющие опытному злоумышленнику, имеющему четкую цель, преодолеть контроль, при этом может требоваться наличие других слабых мест. Например, в значительной части веб-сети используется безопасность транспортного уровня (TLS)/уровень защищенных разъемов secure sockets layer (SSL 3), и более действенные методы в целом недоступны вследствие проблем совместимости.
Максимальный полный	C	0.1	Средство контроля абсолютно эффективно противодействует слабому месту, то есть отсутствуют ошибки и уязвимость, а также отрицательные последствия эксплуатации этой проблемы. Например, тестовая среда может ограничивать операции по доступу к файлам одним рабочим каталогом, что защищает от эксплуатации обхода каталога. Весовой показатель, отличный от нуля, используется для того, чтобы отразить вероятность случайного удаления средства внешнего контроля в будущем, например при изменениях среды программного обеспечения.

Распространенность Prevalence (P) - 1

Распространенность результата поиска определяет частоту появления слабого места данного типа в программном обеспечении. Этот параметр предназначен для использования в обобщенной оценке классов слабых мест, такой как разработка настраиваемых списков слабых мест "Топ-N". При оценке отдельного результата поиска слабого места в условиях автоматического сканирования для данного параметра вероятнее использование значения "Не применяется".

Значение	Код	Вес	Описание
Широкая	W	1.0	Слабое место обнаруживается в большинстве или всем программном обеспечении в связанной среде и может встречаться несколько раз в рамках того же программного пакета.
Высокая	H	0.9	Слабое место встречается весьма часто, но оно не распространено широко.
Общая	C	0.8	Слабость встречается периодически
Ограниченнaя	L	0.7	Слабость встречается редко или никогда
Стандартное значение	D	0.85	Медиана значений "Ограниченнaя", "Общая", "Высокая" и "Широкая".
Неизвестно	UK	0.5	Информации для определения значения этого фактора недостаточно. Возможно, потребуется дальнейший анализ.
Не применяется	NA	1.0	<p>Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом.</p> <p>При выполнении целевой оценки по конкретным результатам поиска слабых мест в приложении, как правило ожидается, что параметр "Распространенность" будет неактуальным, поскольку частоту появления слабого места определяют отдельное приложение и аналитические методы, и в случае наличия большего числа слабых мест многие методы агрегированной оценки будут вырабатывать более высокие оценки.</p>

Распространенность Prevalence (P) - 2

Значение	Код	Вес	Описание
Не применяется	NA	1.0	<p>Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом.</p> <p>При выполнении целевой оценки по конкретным результатам поиска слабых мест в приложении, как правило ожидается, что параметр "Распространенность" будет неактуальным, поскольку частоту появления слабого места определяют отдельное приложение и аналитические методы, и в случае наличия большего числа слабых мест многие методы агрегированной оценки будут вырабатывать более высокие оценки.</p>
Количественное значение	Q		<p>Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов.</p> <p>Точные данные о распространенности могут иметься в ограниченных случаях использования, при условии что пользователь отслеживает данные о слабых местах на низком уровне детализации.</p> <p>Например, разработчик может отслеживать слабое место в рамках семейства продуктов или разработчик ревизии программы может измерять распространенность из анализируемого программного обеспечения по всей клиентской базе. В предыдущей версии CWSS распространенность вычислялась на основании необработанных данных голосования, собираемых по списку Топ-25 за 2011 год, в которых использовались дискретные значения (в интервале от 1 до 4), далее приводимые к интервалу 1–10</p>

ПРИМЕЧАНИЕ. – Поскольку успешная атака на программное обеспечение может быть предпринята даже при наличии единственного слабого места, выбранные весовые показатели не обеспечивают существенного различия между ними.

Metric groups

Группы показателей/метрик

Base Finding Group

- Technical Impact
- Acquired Privilege
- Acquired Privilege Layer
- Internal Control Effectiveness
- Finding Confidence

Attack Surface Group

- Required Privilege
- Required Privilege Layer
- Access Vector
- Authentication Strength
- Authentication Instances
- Level of Interaction
- Deployment Scope

Environmental Group

- Business Impact
- Likelihood of Discovery
- Likelihood of Exploit
- External Control Effectiveness
- Remediation Cost
- Prevalence

ФОРМУЛЫ ОЦЕНКИ CWSS

Оценка CWSS 1.0 может лежать в интервале от 0 до 100. Она рассчитывается следующим образом:

BaseFindingSubscore * AttackSurfaceSubscore * EnvironmentSubscore

Элемент оценки базовых результатов поиска – **Base Finding Subscore** – поддерживает значения в интервале от 0 до 100.

Элементы оценки области атаки и среды – **Attack Surface Subscore** и **Environment Subscore** – поддерживают значения в интервале от 0 до 1.

Оценки базовых результатов поиска

- Base Finding Subscore

Элемент оценки базовых результатов поиска – BaseFindingSubscore – рассчитывается следующим образом:

$$Base = [(10 * TechnicalImpact + 5 * (AcquiredPrivilege + AcquiredPrivilegeLayer) + 5 * FindingConfidence) * f(TechnicalImpact) * InternalControlEffectiveness] * 4.0$$

$$f(TechnicalImpact) = 0 \text{ if } TechnicalImpact = 0; \text{ otherwise } f(TechnicalImpact) = 1.$$

Максимальное возможное значение BaseFindingSubscore составляет 100.

*Определение $f(TechImpact)$ имеет эквивалент в CVSS. Оно используется для обеспечения того, что если Техническое воздействие составляет 0, то другие добавленные параметры непреднамеренно выработают отличную от нуля оценку.

Сочетание **TechnicalImpact** (Техническое воздействие) и **AcquiredPrivilege/AcquiredPrivilegeLayer** (Требуемая привилегия/Уровень требуемой привилегии) дает равный весовой коэффициент, каждый составляющий 40% от BaseFindingSubscore. (Каждый из них генерирует подзначение, максимально равное 10). Существует определенная корректировка параметра Доверие к результатам поиска в размере 20% от Базового (максимальное значение 5).

Элемент **InternalControlEffectiveness** (Эффективность внутреннего контроля) может снизить оценку, возможно до 0 – в зависимости от единственности какого-либо средства внутреннего контроля, которое применялось для данной проблемы. После применения InternalControlEffectiveness возможный интервал результатов составляет 0–25, поэтому используется коэффициент 4.0 для корректировки BaseFindingSubscore в целях приведения его к интервалу 0–100.

Оценки области атаки – Attack Surface Subscore

Элемент оценки области атаки – AttackSurfaceSubscore – рассчитывается следующим образом:

$$[20 * (RequiredPrivilege + RequiredPrivilegeLayer + AccessVector) + 20 * DeploymentScope + 15 * LevelOfInteraction + 5 * AuthenticationStrength] / 100.0$$

Сочетание требуемых привилегий/доступа в совокупности составляет 60% (20%*3) от элемента оценки области атаки;

масштаб развертывания составляет еще 20%;

взаимодействие – 15% и аутентификация – 5%.

Требования к аутентификации не имеют большого значения при том предположении, что требование убедительного доказательства идентичности не будет существенно сдерживать злоумышленника от попыток эксплуатации уязвимости.

Значения этого элемента образуют диапазон от 0 до 100 и далее выполняется их деление на 100.

Оценка среды – Environmental Subscore

Элемент оценки среды – EnvironmentalSubscore – рассчитывается следующим образом:

$$[(10 * \text{BusinessImpact} + 3 * \text{LikelihoodOfDiscovery} + 4 * \text{LikelihoodOfExploit} + 3 * \text{Prevalence}) * f(\text{BusinessImpact}) * \text{ExternalControlEffectiveness}] / 20.0$$

$$f(\text{BusinessImpact}) = 0 \text{ if } \text{BusinessImpact} == 0; \text{ otherwise } f(\text{BusinessImpact}) = 1$$

- Элемент BusinessImpact (Воздействие на деятельность) составляет 50% оценки среды и может привести итоговую оценку к 0.
- Элемент ExternalControlEffectiveness (Эффективность внешнего контроля) всегда не равен нулю (для учета риска его случайного удаления при изменениях среды), однако в противном случае он может оказывать значительное воздействие на итоговую оценку.
- Сочетание элементов вероятности обнаружения и вероятности эксплуатации – LikelihoodOfDiscovery и LikelihoodOfExploit – составляет 35% оценки, а распространенность (Prevalence) – 15%.

Формат представления параметров в векторе CWSS

Формат одного параметра в векторе CWSS имеет вид:

FactorName: Value, Weight

Наименование параметра: Значение, Весовой коэффициент

Например, "**P:NA,1.0**" определяет значение "Не применяется" для параметра "Распространенность" с весовым коэффициентом 1.0. Спецификатор "**AV:P,0.2**" обозначает значение "Физический" для параметра "Вектор доступа" с весовым коэффициентом 0.2.

Параметры разделяются символом прямой косой черты, например:
AV:I,1.0/RP:G,0.9/AS:N,1.0,

в которых содержится перечень значений и весовых коэффициентов для "AV" (Вектор доступа), "RP" (Уровень требуемой привилегии) и "AS" (Сложность аутентификации).

ПРИМЕР

Рассмотрим слабое место, о котором поступило сообщение, где приложение является основным источником дохода компании, то есть оно имеет критически важное значение для деятельности.

Приложение разрешает случайным пользователям интернета создавать учетные записи, используя только адрес электронной почты.

Далее пользователь может эксплуатировать это слабое место для получения привилегий администратора приложения, однако атака не будет успешной, если администратор просматривает отчет о недавней деятельности пользователя, что является общепринятой практикой.

Злоумышленник не сможет получить полный контроль над приложением, но сможет удалять пользователей и данные этого приложения.

Предположим также, что средства контроля для защиты слабых мест отсутствуют, однако устранить эту проблему несложно, и для этого потребуется всего несколько строк кода.

Данная ситуация может быть записана в следующем векторе CWSS:

(TI:H,0.9/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/

RP:G,0.9/RL:A,1.0/AV:I,1.0/AS:N,1.0/IN:T,0.9/SC:A,1.0/

BI:C/0.9,DI:H,1.0/EX:H,1.0/EC:N,1.0/P:NA,1.0)

ПРИМЕР

Данная ситуация может быть записана в следующем векторе CWSS:

(TI:H,0.9/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/
RP:G,0.9/RL:A,1.0/AV:I,1.0/AS:N,1.0/IN:T,0.9/SC:A,1.0/
BI:C/0.9,DI:H,1.0/EX:H,1.0/EC:N,1.0/P:NA,1.0)

Расшифровка вектора:

Техническое воздействие - Высокое

Приобретенная привилегия - Администратор

Уровень приобретенной привилегии -

Приложение

Эффективность внутреннего контроля -

Отсутствует

Доверие к результатам поиска - Подтверждено

Требуемая привилегия - Гостевая

Уровень требуемой привилегии - Приложение

Вектор доступа - Интернет

Сложность аутентификации - Отсутствует

Уровень взаимодействия -

Типовой/ограниченный

Масштаб развертывания - Полное

Воздействие на деятельность - Критическое

Вероятность обнаружения - Высокая

Вероятность эксплуатации - Высокая

Эффективность внешнего контроля - Отсутствует

Распространенность - Не применяется

Итоговая оценка:

96.0 * 0.965 * 1.0 = 92.64 == 92.6

Оценка CWSS для этого вектора составляет 92,6 и получена следующим образом:

BaseSubscore:

$$[(10 * TI + 5 * (AP + AL) + 5 * FC) * f(TI) * IC] * 4.0$$

$$f(TI) = 1$$

$$= [(10 * 0.9 + 5 * (1.0 + 1.0) + 5 * 1.0) * 1 * 1.0] * 4.0$$

$$= [(9.0 + 10.0 + 5.0) * 1.0] * 4.0$$

$$= 24.0 * 4.0$$

$$= 96.0$$

AttackSurfaceSubscore:

$$[20 * (RP + RL + AV) + 20 * SC + 15 * IN + 5 * AS] / 100.0$$

$$= [20 * (0.9 + 1.0 + 1.0) + 20 * 1.0 + 15 * 0.9 + 5 * 1.0] / 100.0$$

$$= [58.0 + 20.0 + 13.5 + 5.0] / 100.0$$

$$= 96.5 / 100.0$$

$$= 0.965$$

EnvironmentSubscore:

$$[(10 * BI + 3 * DI + 4 * EX + 3 * P) * f(BI) * EC] / 20.0$$

$$\text{о } f(BI) = 1$$

$$= [(10 * 1.0 + 3 * 1.0 + 4 * 1.0 + 3 * 1.0) * 1 * 1.0] / 20.0$$

$$= [(10.0 + 3.0 + 4.0 + 3.0) * 1.0] / 20.0$$

$$= 20.0 / 20.0$$

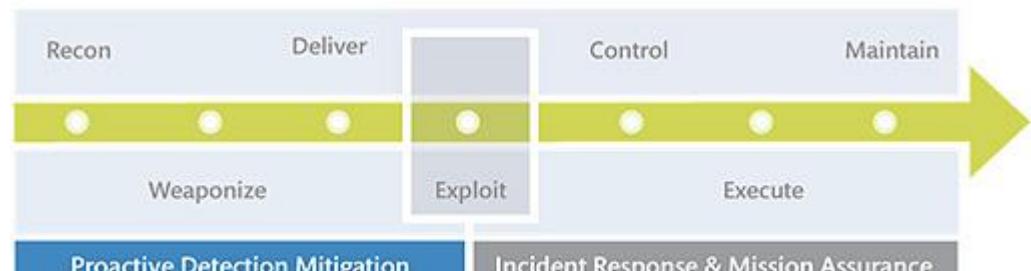
$$= 1.0$$

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ДАННЫМИ БЕЗОПАСНОСТИ. ТАКСОНОМИИ АТАК

CAPEC - COMMON ATTACK PATTERN ENUMERATION AND CLASSIFICATION

ПЕРЕЧЕНЬ И КЛАССИФИКАЦИЯ ОБЩЕИЗВЕСТНЫХ СХЕМ АТАК

К.т.н., доцент ИКТИБ ЮФУ
Князева М.В.



<https://www.mitre.org/capabilities/cybersecurity/threat-based-defense>



CAPEC
capec.mitre.org



CAPEC (Common Attack Pattern Enumeration and Classification)

МСЭ-Т X.1544 (04/2013)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И
БЕЗОПАСНОСТЬ

Обмен информацией, касающейся
кибербезопасности – Обмен информацией
о событии/инциденте/эвристических правилах

Перечень и классификация общеизвестных
схем атак.

Цель перечня и классификации общеизвестных схем атак (CAPEC) состоит в том, чтобы обеспечить общедоступный каталог схем атак, наряду с комплексной схемой и классификационной таксономией.

Рекомендация "Перечень и классификация общеизвестных схем атак (CAPEC)" представляет собой основанную на XML/XSD спецификацию для определения, описания и составления перечня схем атак. Схемы атак являются высокоеффективным средством, позволяющим получать и представлять информацию о подходах, используемых нарушителем защиты. Эти схемы являются описаниями общеизвестных методов использования программного обеспечения. Они выводятся из схем проектных решений, применяемых деструктивным, а не конструктивным образом, и составляются на основе углубленного анализа конкретных примеров реального использования.

CAPEC (Common Attack Pattern Enumeration and Classification)

«Общее перечисление и классификация шаблонов атак»

Важным этапом создания программного обеспечения, устойчивого к угрозам информационной безопасности, является представление возможных шагов злоумышленника и подходов, используемых при компрометации компьютерных систем.

С целью предоставления подобной информации корпорацией MITRE для Министерства национальной безопасности США был создан стандарт «Общее перечисление и классификация шаблонов атак» (**Common Attack Pattern Enumeration and Classification, CAPEC**), который включает в себя открытый каталог шаблонов атак, схему и таксономию атак.

CAPEC предназначен для улучшения защищенности компьютерных систем на всем цикле создания и использования программного обеспечения. Он применяется совместно с несколькими другими стандартами, в том числе со следующими:

- «Общее перечисление слабых мест» (**Common Weakness Enumeration, CWE**) — список общеизвестных слабых мест программных продуктов;
- «Общее перечисление уязвимостей» (**Common Vulnerability Enumeration, CVE**) — список общеизвестных уязвимостей;
- «Перечисление и характеристика атрибутов вредоносных программ» (**Malware Attribute Enumeration and Characterization, MAEC**) — атрибуты вредоносного ПО;
- «Киберразличимое представление» (**Cyber Observable eXpression, CybOX**) — схема определения, сбора, характеристики и передачи событий или свойств состояния.

Основным отличием CAPEC от других релевантных стандартов является то, что в нем описываются не отдельные уязвимости и слабые места, а подходы и методики, используемые атакующими для компрометации информационных систем.

CAPEC (Common Attack Pattern Enumeration and Classification)

CAPEC дает возможность:

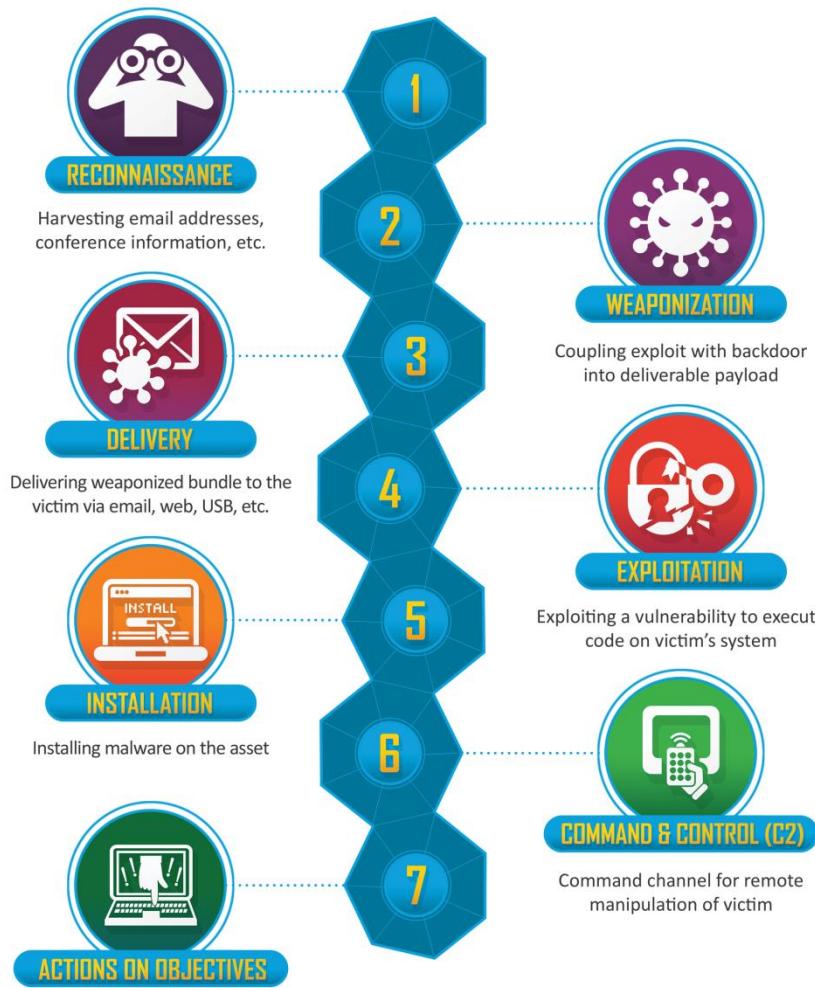
- стандартизировать получение и описание схем атак;
- собирать известные схемы атак в общий перечень, который может согласованным и эффективным образом использоваться сообществом;
- классифицировать схемы атак, с тем чтобы пользователи могли легко определять во всем перечне то подмножество, которое подходит к их условиям;
- с помощью явных ссылок увязать схемы атак и перечни общеизвестных слабых мест (CWE), в которых такие атаки могут быть эффективными.

THREAT-BASED DEFENSE

- Сбор и архивирование артефактов атак, включая инциденты, тактику, данные о нацеливании и оценки потерь.
- Связывание архивных артефактов со стадиями жизненного цикла кибератаки.
- Отслеживание влияния окружающей среды, включая политику, технологические разработки, уязвимости и эксплойты из открытых и конфиденциальных источников.
- Проведение обратного проектирования вредоносных программ для статического и динамического анализа характеристик и поведения вредоносного ПО.
- Анализ собранных данных для выработки гипотез о противниках, их намерениях, а также их тактике, методах и процедурах.
- Использование всех этих элементов для формирования и определения приоритетов защиты и реагирования на инциденты.

Cyber Kill Chain

APT – Advanced Persistent Threat



Анализ киберугроз (Cyber threat intelligence)

Этот тип анализа предоставляет практическую информацию и сигнатуры обнаружения угроз, которые более надежны, чем существующие определения вирусов. После тщательного изучения информации специалисты могут использовать ее для усиления киберзащиты и улучшения способов прогнозирования, предотвращения, обнаружения и реагирования на кибератаки.

Используя жизненный цикл кибератак (впервые сформулированный Lockheed Martin как «цепочку уничтожения») и классический анализ разведывательных данных, аналитики разведки киберугроз разработали структуру, позволяющую лучше понимать и предвидеть действия киберпреступников на каждом этапе атаки.

Threat Profile

Профиль угрозы

Asset/Threat Object

The thing the attacker wants or that the owner needs to protect

Threat Types

STRIDE-LM; CIA;

Attack Surface

The components, interfaces, etc that will be initially attacked;

Attack Vectors - CAPEC

The path or technique the attacker uses to realize the threat;

Threat Actors

The entity who is trying to realize the threat against the asset;

Resultant Condition

Describe what happens if the threat is realized;

Vulnerabilities

Any known vulnerabilities (there may not be any);

Controls Things that will help mitigate or counter the attack.

CAPEC (Common Attack Pattern Enumeration and Classification) – 559 известных шаблонов атак

«Общее перечисление и классификация шаблонов атак»

Уязвимость (vulnerability) [ITU-T X.1500]* - любое слабое место в программном обеспечении, которое могло бы использоваться для нарушения целостности системы или содержащейся в ней информации.

*Рекомендация МСЭ-Т X.1500 (2011 г.), *Методы обмена информацией о кибербезопасности (CYBEX)*.

Случай атаки (attack instance) - конкретная подробно описанная атака против приложения или системы, целью которой являются уязвимые или слабые места в этой системе.

Схема атаки (attack pattern) - обобщение общих подходов в случае атаки, наблюдаемой в неконтролируемых ситуациях в отношении приложений или систем (например, введение запроса SQL, атака через посредника, перехват сеанса связи и т. д.).

Средство (capability): Инструментальное средство оценки, динамической проверки безопасности приложений (DAST-Dynamic Application Security Testing), тестирования на предмет несанкционированного доступа, использования структуры, моделирования угроз, база данных, веб-сайт, инструкция или услуга, которые обеспечивают информацию о случаях и схемах атак.

Слабое место (weakness): Недостаток или несовершенство в коде, проекте, архитектуре или развертывании программного обеспечения, которые в некоторый момент могут стать уязвимыми или могут приводить к появлению других уязвимостей.

ПРИМЕЧАНИЕ. – Одна схема атаки потенциально может включать много различных случаев атак, которые с ней ассоциируются.

Таксономия атак

Под **атакой** на компьютерную систему будем понимать любое воздействие злоумышленника на компьютерную систему (КС) с целью нарушения информационной безопасности, заключающееся в поиске и использовании той или иной уязвимости.

Таксономия атак на компьютерные системы – это классификационная схема, которая структурирует знания о предметной области атак на компьютерные системы (АКС) и определяет отношения между элементами знаний.

Основная цель создания любой таксономии атак состоит в том, чтобы предложить такие классификационные признаки, используя которые можно наиболее точно описать классифицируемые АКС:

- А) осуществлять системное исследование вопросов защиты КС, в частности, структурировать статистические данные об атаках, выделять образцы типовых атак и делать выводы на основании собранных данных.
- Б) формировать сообщения об инцидентах.
- В) разрабатывать компоненты систем защиты информации (например, подсистем обнаружения вторжений).

Схема таксономии: механизм, домен или другие критерии. CAPEC List Version 3.9



Home | About | CAPEC List | Community | News | Search

Understanding how the adversary operates is essential to effective cybersecurity. CAPEC™ helps by providing a comprehensive dictionary of known adversaries to exploit known weaknesses in cyber-enabled capabilities. It can be used by analysts, developers, testers, and educators to advance defenses.

CAPEC List Quick Access

[View CAPEC](#)

[by Mechanisms of Attack](#)

[by Domains of Attack](#)

[by Other Criteria](#)

Search CAPEC

ENHANCED BY Google

Total Attack Patterns: 546



New to CAPEC?

Common Attack Pattern Enumerations and Classifications (CAPEC™) can be overwhelming to someone new to cyber-attack patterns. This page offers tips on how to familiarize yourself with what CAPEC has to offer, before more fully exploring this extensive knowledge base.

Community Engagement

Rest API Working Group

[Join the CWE/CAPEC Rest API WG](#)

User Experience Working Group

[Join the CWE/CAPEC UX WG](#)

CWE/CAPEC Board

[Read the meeting minutes](#)

To get involved, [contact us](#)

Классификационная схема

C (Category) - Категория в CAPEC представляет собой набор шаблонов атак, основанных на некоторой общей характеристистике. Более конкретно, это совокупность паттернов атаки, основанная на эффекте/намерении (в отличие от действий или механизмов, такая агрегация будет паттерном мета-атаки). Агрегация, основанная на эффекте/намерении, не является единственной атакой и, как таковая, не является шаблоном поведения при атаке. Это группировка паттернов на основе некоторых общих критериев.

S (Standard Attack Pattern) - Шаблон атаки стандартного уровня в CAPEC ориентирован на конкретную методологию или технику, используемую в атаке. Это часто рассматривается как отдельная часть полностью выполненной атаки. Стандартный шаблон атаки предназначен для предоставления достаточно подробной информации для понимания конкретной техники и того, как она пытается достичь желаемой цели. Шаблон атаки стандартного уровня — это особый тип более абстрактного шаблона атаки метауровня.

D (Detailed Attack Pattern) - Шаблон подробного уровня атаки в CAPEC обеспечивает низкий уровень детализации, как правило, используя конкретный метод и нацеленный на конкретную технологию, и выражает полный поток выполнения. Подробные шаблоны атак более специфичны, чем шаблоны мета-атак и стандартные шаблоны атак, и часто требуют специального механизма защиты для смягчения реальных атак. Подробный шаблон атаки на уровне часто будет использовать несколько различных шаблонов атаки на стандартном уровне, объединенных в цепочку для достижения цели.

M (Meta Attack Pattern) – Шаблон атаки метауровня в CAPEC — это определенно абстрактная характеристика конкретной методологии или техники, используемой в атаке. Шаблон мета-атаки часто лишен конкретной технологии или реализации и предназначен для обеспечения понимания высокоуровневого подхода. Шаблон атаки метауровня представляет собой обобщение связанной группы шаблонов атаки стандартного уровня. Шаблоны атак метауровня особенно полезны для упражнений по моделированию угроз на уровне архитектуры и дизайна.

Классификационная схема. Примеры

CAPEC-21: Exploitation of Trusted Identifiers

Abstraction: Meta

Extended Description:

- Атаки с использованием доверенных идентификаторов обычно приводят к боковому перемещению злоумышленника в локальной сети, поскольку пользователям часто разрешается аутентифицироваться в системах/приложениях в сети с использованием одного и того же идентификатора. Это позволяет злоумышленнику получать конфиденциальные данные, загружать/устанавливать вредоносное ПО в систему, выдавать себя за законного пользователя в целях социальной инженерии и т. д.
- Атаки на доверенные идентификаторы используют тот факт, что некоторые программы принимают вводимые пользователем данные без проверки их подлинности. Многие процессы на стороне сервера уязвимы для этих атак, потому что обмен данными между серверами не был проанализирован с точки зрения безопасности, или процессы «доверяют» другим системам, поскольку они находятся за брандмауэром. Точно так же уязвимыми могут быть серверы, которые используют легко угадываемые или поддельные схемы для представления цифровой идентификации.
- В таких системах часто используются схемы без криптографии и цифровых подписей (или со взломанной криптографией). Идентификаторы могут быть угаданы или получены из-за недостаточной случайности, плохой защиты (передаются/хранятся в открытом виде), отсутствия целостности (без знака) или неправильной корреляции с точками применения политики управления доступом. Открытые файлы конфигурации и свойств, содержащие конфиденциальные данные, могут дополнительно предоставить злоумышленнику информацию, необходимую для получения этих идентификаторов. Злоумышленник также может «использовать» идентификатор через вредоносную ссылку, как в случае атак с подделкой межсайтовых запросов (CSRF).

Независимо от вектора атаки успешная подделка и олицетворение доверенных учетных данных может привести к тому, что злоумышленник нарушит проверку подлинности, авторизацию и элементы управления аудитом в целевой системе или приложении.

Классификационная схема. Примеры

CAPEC-62: Cross Site Request Forgery

Abstraction: Standard

Description:

- Злоумышленник создает вредоносные веб-ссылки и распространяет их (через веб-страницы, электронную почту и т. д.), как правило, целенаправленно, надеясь побудить пользователей щелкнуть ссылку и выполнить вредоносное действие против какого-либо стороннего приложения.
- В случае успеха действие, встроенное во вредоносную ссылку, будет обработано и принято целевым приложением с уровнем привилегий пользователя. Этот тип атаки использует постоянство и неявное доверие к файлам cookie сеанса пользователя многими современными веб-приложениями.
- В такой архитектуре, как только пользователь аутентифицируется в приложении и в системе пользователя создается файл cookie сеанса, все последующие транзакции для этого сеанса аутентифицируются с использованием этого файла cookie, включая потенциальные действия, инициированные злоумышленником, и просто «используют» существующий файл cookie сеанса.

Классификационная схема. Примеры

CAPEC-467: Cross Site Identification

Abstraction: Detailed

Description:

- Злоумышленник собирает идентифицирующую информацию о жертве через активный сеанс, который браузер жертвы имеет с сайтом социальной сети. У жертвы может быть сайт социальной сети, открытый на одной вкладке, или, возможно, он просто использует функцию «запомнить меня», чтобы поддерживать активность своего сеанса на сайте социальной сети.
- Злоумышленник запускает полезную нагрузку в браузере жертвы, которая прозрачно для жертвы инициирует запрос к сайту социальной сети (например, через доступные API сайта социальной сети) для получения идентифицирующей информации о жертве. Хотя часть этой информации может быть общедоступной, злоумышленник может собирать эту информацию в контексте и может использовать ее для дальнейших атак на пользователя (например, целевого фишинга).
- Есть много других способов, которыми злоумышленник может заставить полезную нагрузку выполнятся в браузере жертвы, главным образом, найдя способ скрыть ее на каком-нибудь авторитетном сайте, который посещает жертва. Злоумышленник также может отправить ссылку жертве по электронной почте и обманным путем заставить жертву перейти по ссылке.
- Эта атака представляет собой атаку с подделкой межсайтовых запросов с двумя основными отличиями. Во-первых, от имени пользователя не выполняется никаких действий, кроме сбора информации. Так что стандартная CSRF-защита в этой ситуации может не сработать. Во-вторых, в этой модели атаки важен характер собираемых данных, т. е. идентификация информации, которую можно получить и использовать в контексте. Этот сбор идентифицирующей информации в режиме реального времени можно использовать в качестве старта для запуска целенаправленных атак социальной инженерии на жертву в реальном времени.

Схема таксономии: Category (C) - Категория Meta Attack Pattern (M) – Мета-описание атаки

CAPEC VIEW: Mechanisms of Attack

View ID: 1000

Status: Stable

Structure: Graph

Downloads: [Booklet](#) | [CSV](#) | [XML](#)

Objective

This view organizes attack patterns hierarchically based on mechanisms that are frequently employed when exploiting a vulnerability. The categories that are members of this view represent the different techniques used to attack a system. They do not, however, represent the consequences or goals of the attacks. There exists the potential for some attack patterns to align with more than one category depending on one's perspective. To counter this, emphasis was placed such that attack patterns as presented within each category use a technique not sometimes, but without exception.

Relationships

The following graph shows the tree-like relationships between attack patterns that exist at different levels of abstraction. At the highest level, categories exist to group patterns that share a common characteristic. Within categories, meta level attack patterns are used to present a decidedly abstract characterization of a methodology or technique. Below these are standard and detailed level patterns that are focused on a specific methodology or technique used.

Show Details:

[Expand All](#) | [Collapse All](#)

1000 - Mechanisms of Attack

-  [Category](#) - A category in CAPEC is a collection of attack patterns based on some common characteristic. More specifically, it is an aggregation of attack patterns based on effect/intent (as opposed to actions or mechanisms, such an aggregation would be a meta attack pattern). An aggregation based on effect/intent is not an actionable attack and as such is not a pattern of attack behavior. Rather, it is a grouping of patterns based on some common criteria.
 -  [Manipulate Human Behavior](#) - (416)
-  [Abuse Existing Functionality](#) - (210)
-  [Manipulate Data Structures](#) - (255)
-  [Manipulate System Resources](#) - (262)
-  [Inject Unexpected Items](#) - (152)
-  [Employ Probabilistic Techniques](#) - (223)
-  [Manipulate Timing and State](#) - (172)
-  [Collect and Analyze Information](#) - (118)
-  [Subvert Access Control](#) - (225)

[BACK TO TOP](#)

Схема таксономии: Detailed Attack Pattern (M) – детальное описание атаки

CAPEC Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks

Home > CAPEC List > CAPEC-220: Client-Server Protocol Manipulation (Version 3.4) ID Lookup:

Home | About | CAPEC List | Community | News | Search

CAPEC-220: Client-Server Protocol Manipulation

Attack Pattern ID: 220 Status: Draft
Abstraction: Standard

Presentation Filter: Complete ▾

Description

An adversary takes advantage of weaknesses in the protocol by which a client and server are communicating to perform unexpected actions. Communication protocols are necessary to transfer messages between client and server applications. Moreover, different protocols may be used for different types of interactions. For example, an authentication protocol might be used to establish the identities of the server and client while a separate messaging protocol might be used to exchange data. If there is a weakness in a protocol used by the client and server, an attacker might take advantage of this to perform various types of attacks. For example, if the attacker is able to manipulate an authentication protocol, the attacker may be able spoof other clients or servers. If the attacker is able to manipulate a messaging protocol, the may be able to read sensitive information or modify message contents. This attack is often made easier by the fact that many clients and servers support multiple protocols to perform similar roles. For example, a server might support several different authentication protocols in order to support a wide range of clients, including legacy clients. Some of the older protocols may have vulnerabilities that allow an attacker to manipulate client-server interactions.

Typical Severity

Medium

Relationships

 Nature	Type	ID	Name
ChildOf	M	272	Protocol Manipulation
ParentOf	D		Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific technique and targeting a specific technology, and expresses a complete execution flow. Detailed attack patterns are more specific than meta attack patterns and standard attack patterns and often require a specific protection mechanism to mitigate actual attacks. A detailed level attack pattern often will leverage a number of different standard level attack patterns chained together to accomplish a goal.
ParentOf	D		
ParentOf	D	274	HTTP Verb Tampering

View Name Domains of Attack **Top Level Categories** Software, Communications

Шаблоны CAPEC (Common Attack Pattern Enumeration and Classification)

Форма представления: “CAPEC-####” (н-р, CAPEC-34: HTTP Response Splitting).

Задача: Поиск уязвимого программного обеспечения.

Решение: используются следующие шаблоны

CAPEC-310 (Scanning for Vulnerable Software)

Attack Pattern ID: 310

Abstraction: Detailed

Description

An attacker engages in scanning activity to find vulnerable software versions or types, such as operating system versions or network services. Vulnerable or exploitable network configurations, such as improperly firewalled systems, or misconfigured systems in the DMZ or external network, provide windows of opportunity for an attacker.

Common types of vulnerable software include unpatched operating systems or services (e.g FTP, Telnet, SMTP, SNMP) running on open ports that the attacker has identified. Attackers usually begin probing for vulnerable software once the external network has been port scanned and potential targets have been revealed.

Typical Severity

Low

Relationships

Nature	Type	ID	Name
ChildOf	Standard Attack Pattern	541	Application Fingerprinting

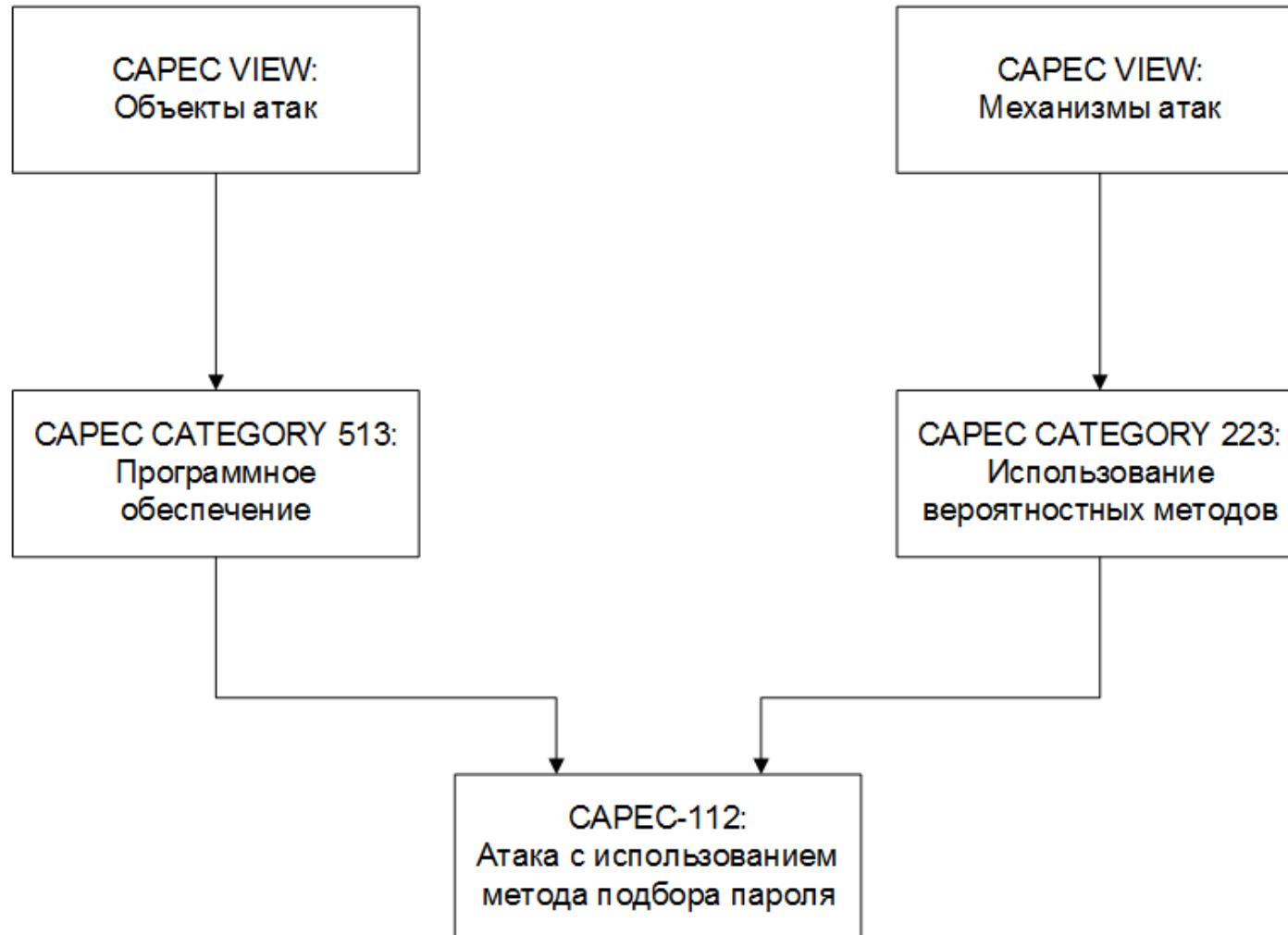
Domains of Attack Software

Mechanisms of Attack Collect and Analyze Information

CAPEC-300 (Port Scanning)

CAPEC-233 (Privilege Escalation)

CAPEC-112 Brute Force



Списки терминов атак, списки категорий атак и категории результатов атак

Ошибки и упущения (Errors and omissions) - ошибочные или опущенные записи, формируемые проектировщиками, программистами, администраторами и т.п.
Забывание устраниить (изменить) пароли по умолчанию, установка некорректной защиты и т.д.

“Троянский конь” (Trojan horse) - компонент аппаратного или программного обеспечения, который имеет незаявленные, как правило, вредоносные эффекты.

Некорректное значение по вызову (Invalid value on call) - передача некорректных значений на системные вызовы для останова функционирования операционной системы.

Использование недокументированных или неизвестных функций (Undocumented or unknown function exploitations) - то же самое, что и общеупотребительное значение.

Атака на доверие (Implied trust attack) - программы неуместно доверяют другим программам.

Сдвиг данных (Data diddling) - незаконная модификация данных, чтобы привести (“обманом”) операционную систему к состоянию, позволяющему получить неправильные результаты.

Списки терминов атак, списки категорий атак и категории результатов атак

Агрегация данных (Data aggregation) — объединение отдельных данных для получения ценной информации.

Обход процесса (Process bypassing) — обход некоторого процесса управления, который имеет неадекватные средства управления.

Переполнение “входа” (Input overflow) — атака программы, которая не контролирует длину входных данных.

Вызванное ошибками неправильное функционирование (Error-induced misoperation) — ошибки, вызванные атакой, приводят к некорректному функционированию системы.

Подавление контроля (Audit suppression) — препятствование правильному функционированию средств аудита.

Отказ, вызванный нажимом (Induced stress failure) — давление на систему, пока она не начинает совершать ошибки.

Аппаратные и системные дефекты (Hardware-system failure-flaw) — используются известные аппаратные или системные дефекты.

Сетевая служба и протокол (Network service and protocol) — используются характеристики сетевых служб.

Распределенные скоординированные атаки (Distributed coordinated attacks) — атакующие распределены, используют для атаки системы промежуточного уровня и действуют согласовано.

Списки терминов атак, списки категорий атак и категории результатов атак

Атаки на межпроцессорное соединение (Interprocess communication attacks) — производится атака на каналы межпроцессорной связи.

Условия гонок (Race conditions) — взаимозависимые последовательности событий прерваны другими событиями, которые разрушают критические зависимости.

Неподходящие умолчания (Inappropriate defaults) — значения параметров по умолчанию “оставляют” систему открытой для атак.

Другая классификационная схема

1. Захват паролей (Stealing passwords) — методы, используемые для получения паролей других пользователей.
2. Социальная инженерия (Social engineering) — получение конфиденциальной информации путем искусственных переговоров.
3. Ошибки и черные ходы (Bugs and backdoors) — использование систем, которые не соответствуют своим спецификациям, или замена программ скомпрометированными версиями.
4. Ошибки аутентификации (Authentication failures) — нарушение механизмов, используемых для аутентификации.
5. Ошибки протоколов (Protocol failures) — протоколы ненадлежащим образом разработаны или реализованы.
6. Утечка информации (Information leakage) — получение информации, которая необходима администраторам, для корректного функционирования сети, но также может использоваться злоумышленниками.
7. Отказ в обслуживании (Denial of service) — усилия, направленные на создание препятствий пользователям в использовании их систем.

Методы компьютерных злоупотреблений

- внешняя кража информации (подглядывание за экраном компьютера);
- внешнее злоупотребление ресурсами (порча дисковода);
- маскарад (регистрация и воспроизведение передачи информации по сети);
- программы-вредители (установка злонамеренной программы);
- обход аутентификации или авторизации (раскрытие пароля);
- злоупотребление полномочиями (фальсификация записей);
- злоупотребление вследствие бездействия (преднамеренно плохое администрирование);
- косвенное злоупотребление (использование другой системы для создания злонамеренной программы).

Пример описания шаблона атаки CAPEC

CAPEC-34

Название

Критичность

Описание

Необходимые предпосылки атаки

Вероятность эксплуатации

Метод атаки

HTTP Response Splitting

Разделение HTTP-ответов.

Высокая.

Разделение HTTP-ответов приводит к тому, что уязвимый веб-сервер отвечает на вредоносный запрос, отправляя клиенту HTTP-ответ таким образом, что он интерпретируется в браузере как два отдельных ответа вместо одного. Это возможно, когда контролируемый пользователем ввод используется в составе заголовков ответов. Злоумышленник может заставить жертву интерпретировать введенный Заголовок как ответ на второй фиктивный запрос, в результате чего созданное содержимое будет отображаться клиентом и, возможно, кэшироваться на промежуточных прокси-серверах или самом клиенте. Чтобы добиться разделения HTTP-ответа на уязвимом веб-сервере, злоумышленник:

- 1.Находит такие данные для ввода, которые приводят к произвольному внедрению HTTP-заголовка.
- 2.Производит вредоносный ввод, состоящий из данных, необходимых для того, чтобы завершить исходный ответ (например, \r\n\r\n) и начать второй ответ с заголовками, контролируемыми злоумышленником.
- 3.Вынуждает жертву отправить на уязвимый сервер два HTTP-запроса. Первый запрос состоит из вредоносного ввода, который будет использоваться как часть заголовков HTTP-ответов, а второй является фиктивным запросом, чтобы жертва интерпретировала вторую часть разделенного ответа как принадлежащую второму HTTP-запросу.

Пользователь может контролировать входные данные, которые могут использоваться как часть HTTP-заголовка.

Возможность злоумышленника внедрять произвольные строки в HTTP-заголовок.
Недостаточные проверки входных данных.

Средняя.

Внедрение, манипуляция протоколом.

Пример описания шаблона атаки CAPEC

CAPEC-34	HTTP Response Splitting
Название	Разделение HTTP-ответов.
Примеры сценария	Уязвимость CVE-2006-0207.
Компетенции злоумышленника	Высокие, злоумышленник должен иметь глубокое понимание протокола HTTP.
Необходимые злоумышленнику ресурсы	Нет.
Признаки атаки	Единственный признак – несколько ответов на один запрос в логах, однако это сложно заметить без анализатора журнала. Чтобы избежать разделения HTTP-ответов, приложение не должно доверять вводу пользователя при формировании выходного потока ответов (заголовков или тела). Разделение ответов происходит за счет внедрения последовательностей CR-LF и дополнительных заголовков. Все данные, поступающие от пользователя и используемые в качестве части заголовков HTTP-ответов, должны подвергаться строгой проверке (валидации).
Способ предотвращения	Исполнение несанкционированного кода или команд. Вытекающие последствия – повышение привилегий.
Цель и последствия	Атаки разделения HTTP-ответа происходят там, где сценарий сервера внедряет управляемые пользователем данные в заголовки HTTP-ответа. Обычно это происходит, когда скрипт встраивает такие данные в URL-адрес перенаправления в ответ перенаправления (код статуса HTTP 3xx), или когда сценарий включает такие данные в cookie ответа.
Описание контекста	Управляемый пользователем ввод, который является частью выходных заголовков HTTP-ответов.
Вектор атаки	Закодированный HTTP-заголовок и данные, разделенные соответствующими последовательностями CR-LF. Вводимые данные должны состоять из корректных HTTP-заголовков, а также скрипта (обычно JavaScript), который будет включен в текст HTML.
Атакующая строка	Вызовы API в приложении, которые формируют выходные заголовки HTTP-ответов.
Зона активации	CWE-113, CWE-74, CWE-697, CWE-707, CWE-713.
Связанные недостатки	

Пример описания шаблона атаки CAPEC-34

CAPEC-34: HTTP Response Splitting

Attack Pattern ID: 34

Abstraction: Detailed

Status: Draft

Presentation Filter: Complete ▾

Description

This attack uses a maliciously-crafted HTTP request in order to cause a vulnerable web server to respond with an HTTP response stream that will be interpreted by the client as two separate responses instead of one. This is possible when user-controlled input is used unvalidated as part of the response headers. The target software, the client, will interpret the injected header as being a response to a second request, thereby causing the maliciously-crafted contents be displayed and possibly cached.

Likelihood Of Attack

Medium

Typical Severity

High

Relationships

Nature	Type	ID	Name
ChildOf	S	220	Client-Server Protocol Manipulation
PeerOf	D	105	HTTP Request Splitting

View Name

[Domains of Attack](#)

[Mechanisms of Attack](#)

Top Level Categories

[Software, Communications](#)

[Abuse Existing Functionality](#)

Execution Flow

Explore

- Spider:** Using a browser or an automated tool, an adversary follows all public links on a web site. They record all the links, the forms and all potential user-controllable input points for the web application.

Techniques

Use a spidering tool to follow and record all links and analyze the web pages to find entry points. Make special note of any links that include parameters in the URL, forms found in the pages (like file upload, etc.).

Use a proxy tool to record all links visited during a manual traversal of the web application.

Use a browser to manually explore the website and analyze how it is constructed. Many browsers' plugins are available to facilitate the analysis or automate the discovery.

Пример описания шаблона атаки CAPEC-34

Explore

- Spider:** Using a browser or an automated tool, an adversary follows all public links on a web site. They record all the links, the forms and all potential user-controllable input points for the web application.

Techniques

Use a spidering tool to follow and record all links and analyze the web pages to find entry points. Make special note of any links that include parameters in the URL, forms found in the pages (like file upload, etc.).

Use a proxy tool to record all links visited during a manual traversal of the web application.

Use a browser to manually explore the website and analyze how it is constructed. Many browsers' plugins are available to facilitate the analysis or automate the discovery.

Experiment

- Attempt variations on input parameters:** The adversary injects the entry points identified in the Explore Phase with response splitting syntax and variations of payloads to be acted on in the additional response. They record all the responses from the server that include unmodified versions of their payload.

Techniques

Use CR\LF characters (encoded or not) in the payloads in order to see if the HTTP header can be split.

Use a proxy tool to record the HTTP responses headers.

Exploit

- Cross-Site Scripting:** As the adversary succeeds in exploiting the vulnerability, they can choose to attack the user with Cross-Site Scripting. The possible outcomes of such an attack are described in the Cross-Site Scripting related attack patterns.

Techniques

Inject cross-site scripting payload preceded by response splitting syntax (CR/LF) into user-controllable input identified as vulnerable in the Experiment Phase.

- Cache poisoning:** The adversary decides to target the cache server by forging new responses. The server will then cache the second request and response. The cached response has most likely an attack vector like Cross-Site Scripting; this attack will then be served to many clients due to the caching system.

Techniques

The adversary decides to target the cache server by forging new responses. The server will then cache the second request and response. The cached response has most likely an attack vector like Cross-Site Scripting; this attack will then be served to many clients due to the caching system.

Prerequisites

User-controlled input used as part of HTTP header

Ability of adversary to inject custom strings in HTTP header

Insufficient input validation in application to check for input sanity before using it as part of response header

Пример описания шаблона атаки CAPEC-34

▼ Prerequisites

User-controlled input used as part of HTTP header

Ability of adversary to inject custom strings in HTTP header

Insufficient input validation in application to check for input sanity before using it as part of response header

▼ Skills Required

[Level: High]

The adversary needs to have a solid understanding of the HTTP protocol and HTTP headers and must be able to craft and inject requests to elicit the split responses.

▼ Resources Required

None: No specialized resources are required to execute this type of attack.

▼ Indicators

The only indicators are multiple responses to a single request in the web logs. However, this is difficult to notice in the absence of an application filter proxy or a log analyzer. There are no indicators for the client

▼ Consequences

Scope	Impact	Likelihood
Confidentiality	Execute Unauthorized Commands	
Integrity		
Availability		
Confidentiality		
Access Control	Gain Privileges	
Authorization		

▼ Mitigations

To avoid HTTP Response Splitting, the application must not rely on user-controllable input to form part of its output response stream. Specifically, response splitting occurs due to injection of CR-LF sequences and additional headers. All data arriving from the user and being used as part of HTTP response headers must be subjected to strict validation that performs simple character-based as well as semantic filtering to strip it of malicious character sequences and headers.

▼ Example Instances

In the PHP 5 session extension mechanism, a user-supplied session ID is sent back to the user within the Set-Cookie HTTP header. Since the contents of the user-supplied session ID are not validated, it is possible to inject arbitrary HTTP headers into the response body. This immediately enables HTTP Response Splitting by simply terminating the HTTP response header from within the session ID used in the Set-Cookie directive. See also: [CVE-2006-0207](#)

▼ Related Weaknesses

1 CWE-ID Weakness Name

[113](#) Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')

Пример описания шаблона атаки CAPEC-34

Related Weaknesses

CWE-ID	Weakness Name
113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')
697	Incorrect Comparison
707	Improper Neutralization
713	OWASP Top Ten 2007 Category A2 - Injection Flaws
74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Taxonomy Mappings

Relevant to the WASC taxonomy mapping

Entry ID	Entry Name
25	HTTP Response Splitting

Relevant to the OWASP taxonomy mapping

Entry Name
HTTP Response Splitting

References

[REF-1] G. Hoglund and G. McGraw. "Exploiting Software: How to Break Code". Addison-Wesley. 2004-02.

Content History

Page Last Updated or Reviewed: December 17, 2020

Таксономии инцидентов. Язык описания инцидентов.

Таксономия инцидентов определяет процесс, “связывающий” атакующих с конечными целями атак. Взаимосвязь между атакующими и целями атак устанавливается в виде следующей последовательности:

Атакующие ⇒ Средства ⇒ Доступ ⇒ Результаты ⇒ Цели.

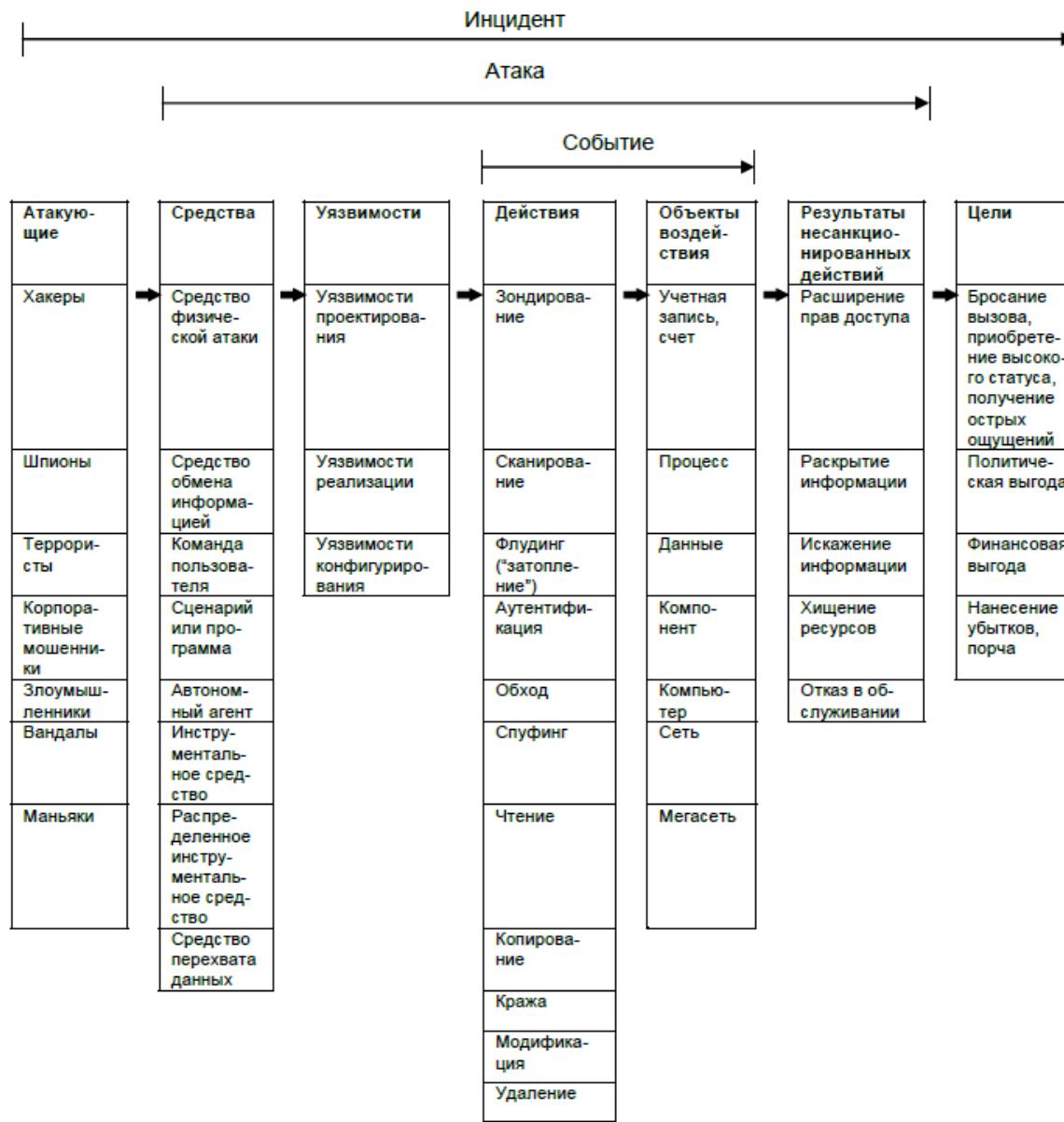
Эта таксономия показывает отношения событий, атак и инцидентов.

Она предполагает, что достижение целей атаки может предотвращаться посредством создания препятствий атакующим в выполнении любой законченной цепочки, состоящей из семи элементов.

Создание препятствий может осуществляться, например, по следующим направлением:

- изучение пользователей, которые могут являться потенциальными атакующими;
- периодическое обследование системы на наличие инструментальных средств атаки;
- исправление обнаруженных уязвимостей системы;
- усиление механизмов управления доступом для предотвращения действий атакующего по доступу к объектам воздействий (например, учетным записям);
- шифрование файлов для предотвращения одного из результатов несанкционированных действий — раскрытия информации;
- реализация общественных образовательных программ для предотвращения достижения целей атакующих.

Таксономия отношения событий, атак и инцидентов.



Structured Threat Information eXpression — STIX™

A Structured Language for Cyber Threat Intelligence Information.

Структурированный язык для описания угроз ИБ

APT1: пример китайской группировки, занимавшейся промышленным кибершпионажем



*К.т.н., доцент ИКТИБ ЮФУ
Князева Маргарита Владимировна*

STIX (Structured Threat Information eXpression)



STIX (Structured Threat Information eXpression) - стандарт, используемый для предоставления унифицированной информации о киберугрозах (CTI).

CIT (Cyber threat intelligence) - is information about threats and threat actors that helps mitigate harmful events in cyberspace. Cyber threat intelligence sources include open source intelligence, social media intelligence, human Intelligence, technical intelligence or intelligence from the deep and dark web.

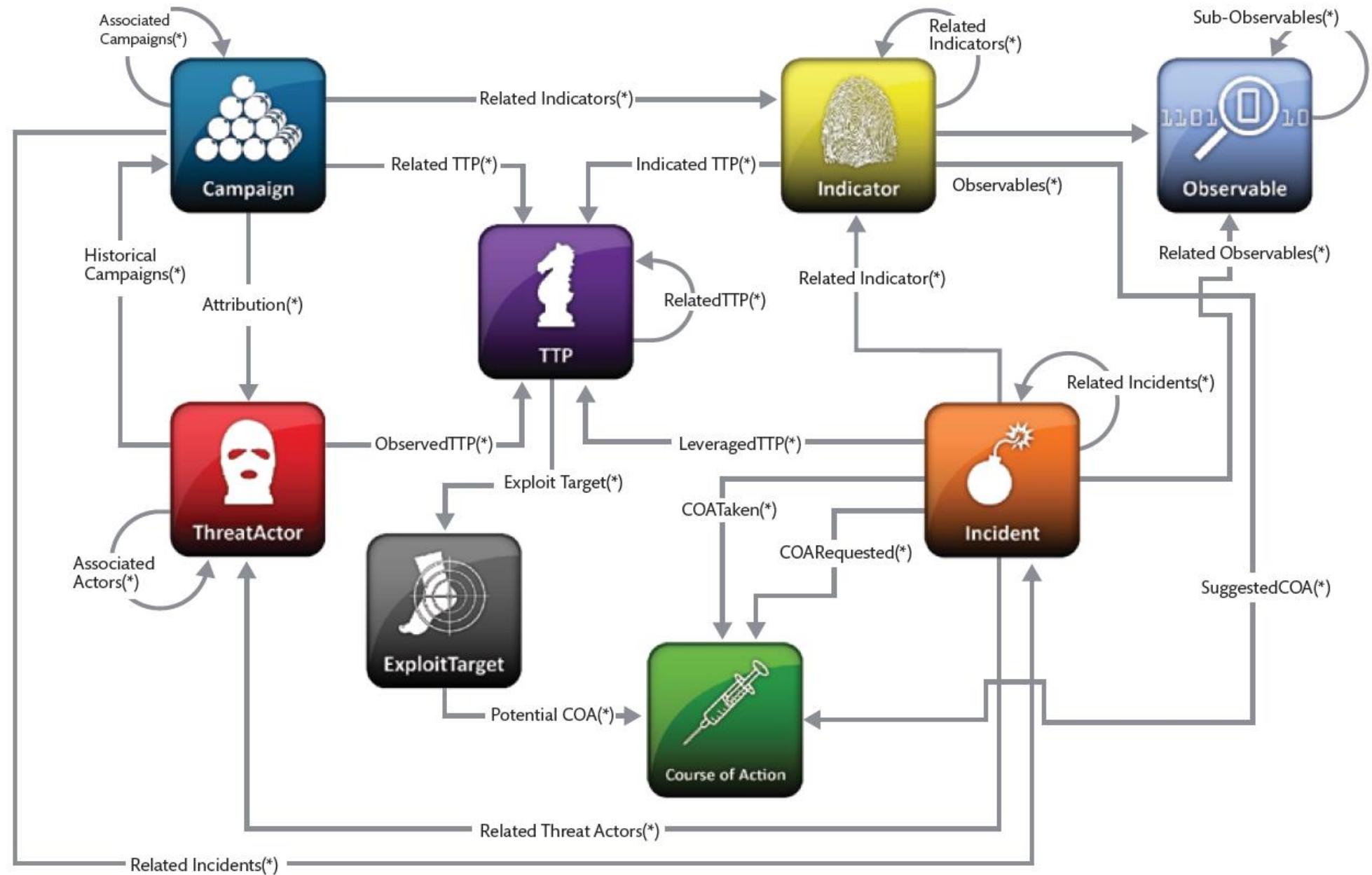
Он имеет хорошие описательные характеристики: с его помощью можно очень детально описать угрозу, все ее взаимосвязи, технические артефакты, при этом результат будет пригоден как для анализа человеком, так и машиной.

STIX является языком описания для обмена данными Threat Intelligence (Интеллектуальный анализ угроз безопасности) и вводит набор сущностей, а также определяет возможные типы взаимосвязей между ними.

Согласно спецификации, STIX чаще всего использует формат JSON, схемы находятся в публичном репозитории на GitHub.

STIX описывает данные об угрозах как связный граф, где узлами являются **SDO (STIX Domain Objects)**, то есть доменные объекты, а ребрами — **SRO (STIX Relationship objects)**, как атрибутивные связи между доменными объектами.

Архитектура STIX - Objects





Attack Pattern (Шаблон Атаки)

A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.



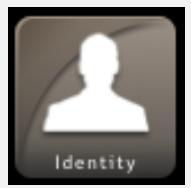
Campaign (Кампания)

A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.



Course of Action (Курс действий)

An action taken to either prevent an attack or respond to an attack.



Identity (Личность, сущность)

Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.



Indicator (Индикатор)

Contains a pattern that can be used to detect suspicious or malicious cyber activity.



Intrusion Set (Множество вторжений)

A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.



Malware (Вирусы)

A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.



Observed Data
(Анализируемая
инф.)

Conveys information observed on a system or network (e.g., an IP address).



Report (Отчеты)

Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.



Threat Actor
(Актор,
злоумышленник)

Individuals, groups, or organizations believed to be operating with malicious intent.



Tool
(Инструменты)

Legitimate software that can be used by threat actors to perform attacks.



Vulnerability
(Уязвимости)

A mistake in software that can be directly used by a hacker to gain access to a system or network.

STIX(Structured Threat Information eXpression)

STIX описывает данные об угрозах как связный граф, где узлами являются **SDO (STIX Domain Objects)**, а ребрами — **SRO (STIX Relationship objects)**.

В качестве **SDO** STIX определяет следующие сущности:

Схема атаки (Attack pattern) — описывает подход (TTP), который использовал злоумышленник для взлома своей цели. Эта сущность используется для классификации атак, обобщения конкретных атак в соответствии со схемами, которым они следуют, и предоставления подробной информации о том, как атаки выполняются.

Вредоносная кампания (Campaign) — описывает последовательность вредоносных поведенческих признаков, которые возникают на протяжении определенных промежутков времени.

План действий (Course of action) — описывает меры, которые нужно принять, чтобы избежать или противостоять атаке.

Личность (Identity) — описывает персоны, организации либо их группы.

Индикатор (Indicator) — описывает технические вредоносные артефакты, которые могут быть использованы для обнаружения вредоносной активности (например, IP-адреса, домены, хеши, ключи реестра).

Intrusion set — описывает набор поведенческих признаков и ресурсов с общими свойствами, которые, вероятней всего, подконтрольны одной организации. Ключевое отличие от Campaign в том, что последняя обычно представляет собой вредоносную активность, направленную на конкретную цель и длится в течение ограниченного промежутка времени, тогда как Intrusion set длится продолжительное время, может участвовать в нескольких Campaigns и иметь несколько целей.

STIX(Structured Threat Information eXpression)

STIX описывает данные об угрозах как связный граф, где узлами являются **SDO (STIX Domain Objects)**, а ребрами — **SRO (STIX Relationship objects)**.

В качестве **SDO** STIX определяет следующие сущности:

Вредоносное ПО (Malware) — описывает экземпляры вредоносного ПО.

Объект наблюдения (Observed data) — описывает не вредоносные технические артефакты.

Отчет (Report) — описывает в понятном виде какую-либо угрозу, вредоносную группировку, их TTP, жертв. Своего рода аналитическая сводка, позволяющая понять суть угрозы, ее опасность, вредоносное ПО, используемые техники, тактики и процедуры, применяемые атакующей стороной.

Злоумышленник (Threat actor) — описывает персон, группы или организации, которые действуют со злым умыслом. Если коротко, злоумышленники и хакеры. Именно злой умысел в мотивации этой сущности отличает ее от Identity.

Инструмент (Tool) — описывает легитимное ПО, которое может быть использовано для осуществления атак. Отличие этой сущности от Malware именно в том, что это легитимный софт, например, nmap или RDP, VNC.

Уязвимость (Vulnerability) — описывает недостатки в требованиях, логике, дизайне, реализации ПО или железа, которые могут быть проэксплуатированы и негативно повлиять на конфиденциальность, целостность или доступность системы.

Индикаторы компрометации

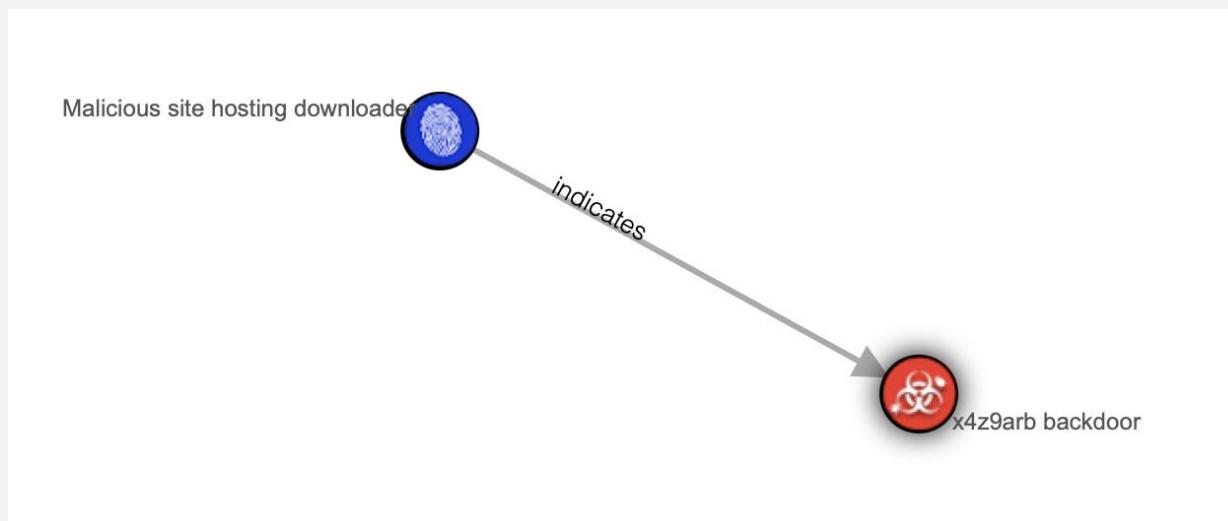


STIX(Structured Threat Information eXpression) - Примеры

Пример 1. Описывается индикатор компрометации <http://x4z9arb.cn/4712/> типа URL и его связь (атрибуция) с вредоносным ПО x4z9arb backdoor.

При этом явно видно, что индикатор — это сайт, на котором располагается вредоносный загрузчик (downloader), в данном случае вредонос x4z9arb backdoor.

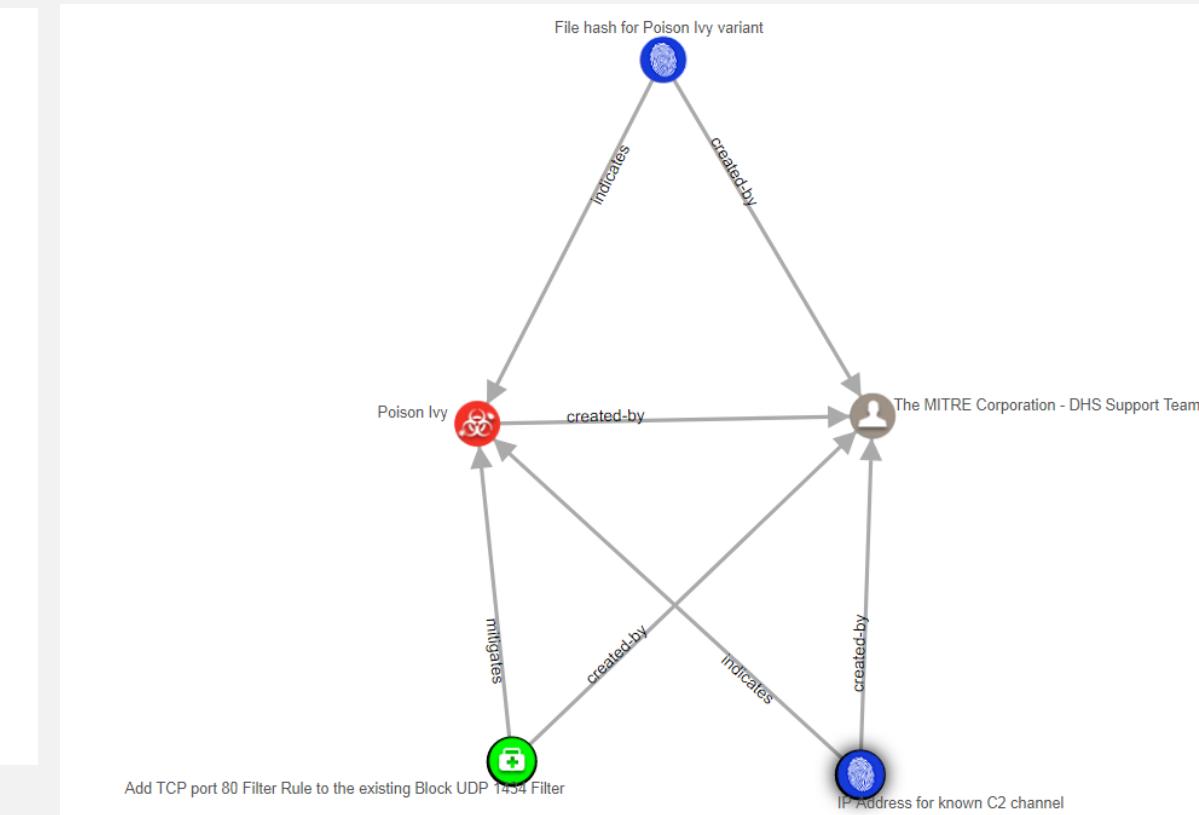
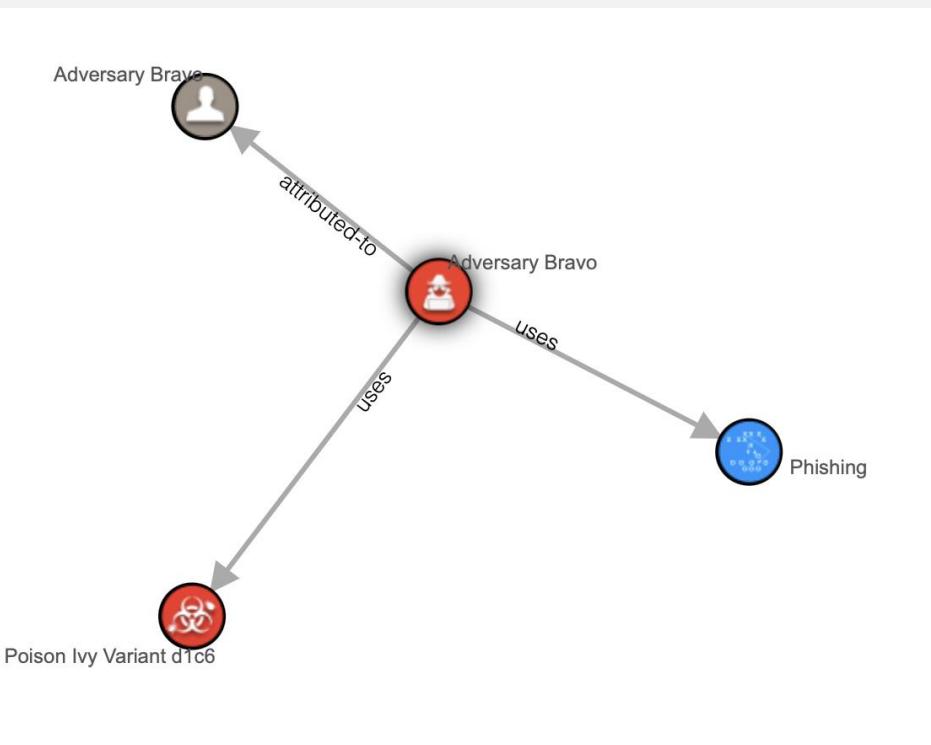
Что это значит для аналитика? Если мы обнаружим следы присутствия (индикатор компрометации <http://x4z9arb.cn/4712/>) в инфраструктуре компании, то можем сделать вывод, что имеем дело с вредоносным ПО x4z9arb backdoor. Дальнейшие шаги обычно зависят от вредоносности ПО, попавшего внутрь инфраструктуры. Для его анализа существует множество баз, например, Malpedia (<https://malpedia.caad.fkie.fraunhofer.de/>)



STIX (Structured Threat Information eXpression) - Примеры

Пример 2. Описаны связи между злоумышленником Adversary Bravo, используемой им техникой атаки — фишингом — и вредоносным ПО Poison Ivy Variant d1c6.

В этом случае при обнаружении в инфраструктуре вредоносного ПО PoisonIvy вариант d1c6 такая структура фида с взаимосвязями поможет понять, что подобным вредоносным ПО пользуется злоумышленник.



APT1: разоблачение китайской организации, занимавшейся промышленным кибершпионажем

- APT1 представляет из себя организацию, которая осуществляла операции кибершпионажа против компаний обширного диапазона деятельности, причем мы зафиксировали, что эти атаки велись, по крайней мере, с 2006 г.
- APT1 представляет из себя одно из подразделений Народно-освободительной армии Китая (НОАК) (2nd Bureau of the People's Liberation army (PLa)).
- Начиная с 2006 г., Mandiant обнаружила, что APT1 скомпрометировала 141 организацию, которые охватывают 20 основных отраслей промышленности. Из 141-ой компании-жертвы APT1, в 87% случаев штаб-квартиры этих компаний находились в англо-говорящих странах.
- APT1 имеет четко определенную методологию атаки, которая была отточена годами и предназначалась для похищения больших объемов ценной интеллектуальной собственности.
- Как только группа APT1 получала доступ в сеть жертвы, они время от времени возвращались в эту скомпрометированную сеть, в течении нескольких месяцев или лет и похищала широкий спектр информации интеллектуальной собственности, включая технологические проекты, данные закрытых процессов производства, результаты испытаний, бизнес-планы, электронные письма и т. д.

APT1: разоблачение китайской организации, занимавшейся промышленным кибершпионажем

- APT1 использует некоторые инструменты и техники, которые мы прежде не наблюдали в арсенале других групп, включая два инструмента, которые предназначены для кражи электронной почты — GETMAIL и MAPIGET.
- APT1 поддерживают установленный ранее доступ к компьютерным сетям жертв в среднем 356 дней. Самый длинный период времени, на который APT1 смогли получить доступ к скомпрометированной сети был 1764 дня или 4 года и 10 месяцев.
- Среди других масштабных краж, которые были предприняты APT1, мы наблюдали один случай, при котором было похищено 6,5 терабайт данных у одной организации, в течении 10 месяцев атаки.
- В первом месяце 2011 г., APT1 успешно скомпрометировали, по крайней мере, 17 новых жертв, которые работали в 10 различных отраслях промышленности.
- APT1 использовала в своей деятельности 937 командных C&C сервера, с которыми связаны 849 различных IP-адресов в 13 странах мира. Большинство из этих 849 адресов были зарегистрированы в Китае (709) и США (109).
- APT1 использовали доменные имена, которые транслировались в 988 уникальных IP-адресов.

APT1: разоблачение китайской организации, занимавшейся промышленным кибершпионажем

В стремлении подчеркнуть, что существуют физические лица, которые непосредственно управляют компьютерами, Mandiant выявляет три персоны, которые связаны с деятельностью APT1.

- Первый человек, “UglyGorilla”, принял активное участие в операциях APT1, начиная с 2004 г. Его деятельность включала в себя регистрацию доменов для APT1, а также он является автором вредоносного ПО, которое используется APT1 при выполнении атак. «UglyGorilla» публично выразил свою заинтересованность в участии в “кибер-войсках” Китая в Январе 2004 г.
- Второй персонаж, которого мы называем “DOTA”, зарегистрировал десятки учетных записей электронной почты, которые использовались для проведения атак с использованием фишинга и методов социальной инженерии. “DOTA” использовал несколько телефонных номеров Шанхая, в процессе регистрации этих аккаунтов.
- Оба персонажа “UglyGorilla” и “DOTA” использовали те же доменные и IP-адреса, которые используются APT1.

APT1: разоблачение китайской организации, занимавшейся промышленным кибершпионажем

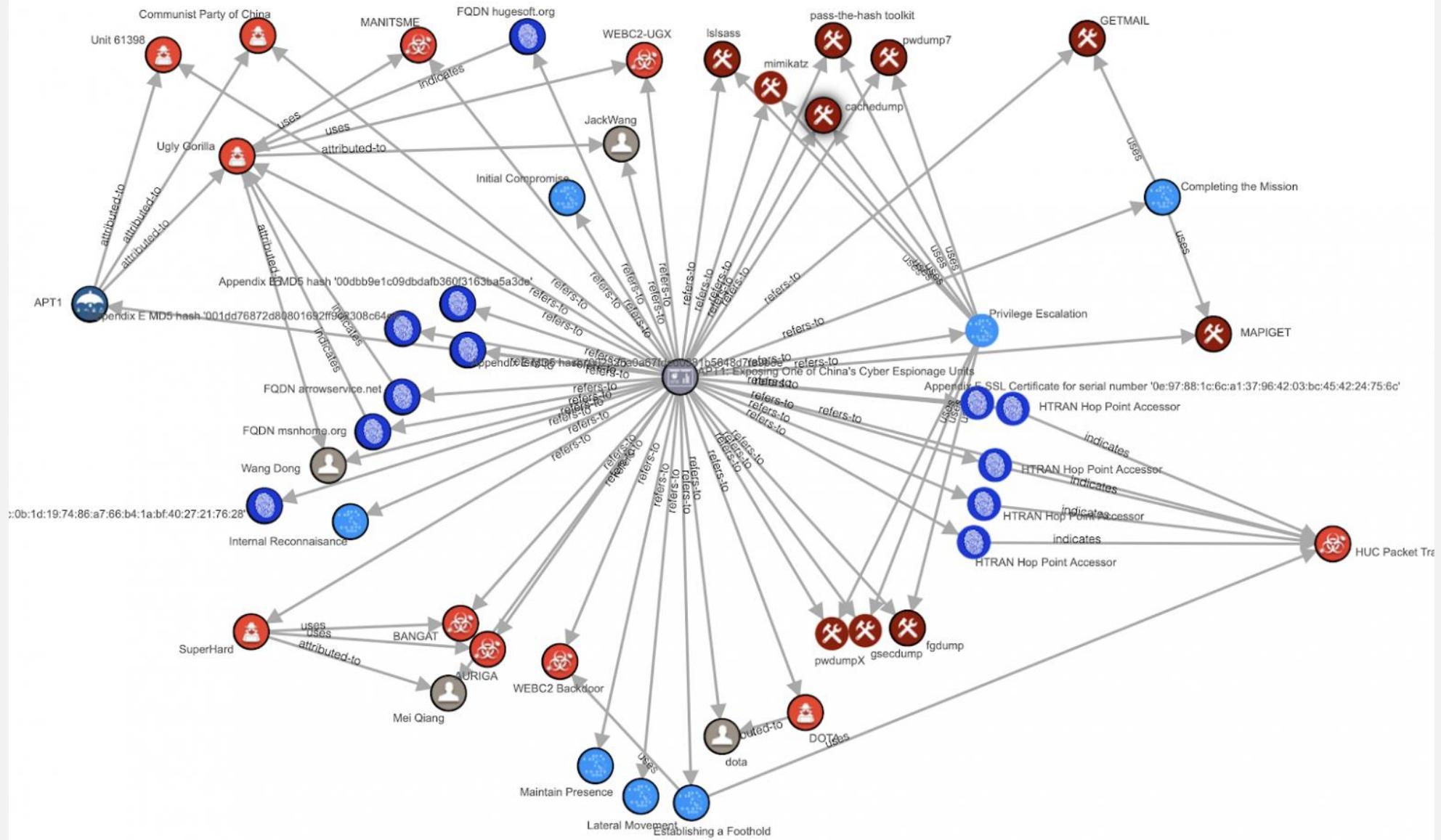
Mandiant опубликовала более 3 тыс. показателей компрометации, которые должны помочь в защите от операций, проводимых APT1. В частности, эта информация включает:

- Около 3 тыс. APT1 индикаторов, включая имена доменов, IP-адреса и хэши MD5 вредоносного ПО.
- Примеры индикаторов компрометации (Indicators of Compromise) и подробные описания более сорока семейств вредоносного ПО.
- Тринадцать сертификатов шифрования X.509, которые использовались APT1.
- В 2011 года APT1 успешно скомпрометировали 17 новых жертв, работавших в 10 различных отраслях промышленности. Группа оставалась активной в скомпрометированной сети каждой жертвы, в среднем на год, после даты первоначальной компрометации, и APT1 совершил эти 17 новых вторжений при одновременном сохранении доступа к сетям своих предыдущих жертв.

STIX(Structured Threat Information eXpression) – Расследование APT1

Пример 3. Исследование — отчета о деятельности вредоносной группировки APT1. Ссылка на JSON:

https://oasis-open.github.io/cti-documentation/examples/example_json/apt1.json



JSON (JavaScript Object Notation) синтаксис

В качестве значений в JSON могут быть использованы:

- **запись** — это неупорядоченное множество пар **ключ: значение**, заключённое в фигурные скобки «{ }». Ключ описывается **строкой**, между ним и значением стоит символ «:». Пары **ключ-значение** отделяются друг от друга запятыми.
- **массив** (одномерный) — это упорядоченное множество **значений**. Массив заключается в квадратные скобки «[]». Значения разделяются запятыми. Массив может быть пустым, то есть не содержать ни одного значения. Значения в пределах одного массива могут иметь разный тип.
- **строка** — это упорядоченное множество из нуля или более символов, заключённое в двойные кавычки.

```
{  
    "type": "malware",  
    "is_family": true,  
    "spec_version": "2.1",  
    "id": "malware--591f0cb7-d66f-4e14-a8e6-5927b597f920",  
    "name": "Poison Ivy",  
    "description": "Poison Ivy is a remote access tool, first released in 2005 but unchanged  
since 2008. It includes features common to most Windows-based RATs, including key  
logging, screen capturing, video capturing, file transfers, system administration, password  
theft, and traffic relaying.",  
    "malware_types": [  
        "remote-access-trojan"  
    ],  
},
```

Индикаторы

```
"type": "indicator",
  "spec_version": "2.1",
  "pattern_type": "stix",
  "id": "indicator--031778a4-057f-48e6-9db9-c8d72b81ccd5",
  "created": "2015-05-15T09:12:16.432Z",
  "modified": "2015-05-15T09:12:16.432Z",
  "name": "HTRAN Hop Point Accessor",
  "description": "Test description.",
  "pattern": "[ipv4-addr:value = '223.166.0.0/15']",
  "indicator_types": [
    "malicious-activity"
```

*HTran — это отражатель соединений, предназначенный для перенаправления TCP-трафика, предназначенного для одного хоста, на альтернативный хост. Цель этого типа инструмента — скрыть истинный источник или место назначения интернет-трафика в ходе хакерской деятельности.

Индикаторы

```
"type": "indicator",
  "spec_version": "2.1",
  "pattern_type": "stix",
  "id": "indicator--8390fd29-24ed-45d4-84d7-c5e5feaf195d",
  "created": "2015-05-15T09:12:16.432Z",
  "modified": "2015-05-15T09:12:16.432Z",
  "name": "FQDN arrowservice.net",
  "description": "Test description.",
  "pattern": "[domain-name:value = 'arrowservice.net']",
  "indicator_types": [
    "malicious-activity"
  ]
```

*FQDN (от англ. Fully Qualified Domain Name — «полностью определённое имя домена», иногда сокращается до «полное имя домена») — имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS.

Различие между FQDN и доменным именем появляется при именовании доменов второго, третьего уровня и так далее. Для получения FQDN требуется обязательно указать в имени домены более высокого уровня (например, sample является доменным именем, однако FQDN имя выглядит как sample.gtw-02.office4.example.com.). В DNS-записях доменов (для перенаправления, почтовых серверов и так далее) всегда используются FQDN.

Индикаторы

```
"type": "indicator",
  "spec_version": "2.1",
  "pattern_type": "stix",
  "id": "indicator--8d12f44f-8ac0-4b12-8b4a-3699ca8c9691",
  "created": "2015-05-15T09:12:16.432Z",
  "modified": "2015-05-15T09:12:16.432Z",
  "name": "Appendix E MD5 hash '001dd76872d80801692ff942308c64e6"",
  "description": "Test description.",
  "pattern": "[file:hashes.md5 = '001dd76872d80801692ff942308c64e6']",
  "indicator_types": [
    "malicious-activity"
```

* MD5 (англ. Message Digest 5) — 128-битный алгоритм хеширования.

Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности. Широко применялся для проверки целостности информации и хранения хешей паролей.

Создатели вредоносных программ используют массу разных методов, чтобы скрыть вредоносное ПО от антивирусных средств и статических-динамических анализаторов. Антивирусы для поиска «родственных» семплов используют продвинутые алгоритмы хеширования. На практике в большинстве случаев существующая база или ядро вредоноса повторно используется для создания новой разновидности malware.

Индикаторы

```
"type": "indicator",
  "spec_version": "2.1",
  "pattern_type": "stix",
  "id": "indicator--b3b6b540-d838-41e2-853b-005056c00008",
  "created": "2015-05-15T09:12:16.432Z",
  "modified": "2015-05-15T09:12:16.432Z",
  "name": "Appendix F SSL Certificate for serial number  
(Negative)4c:0b:1d:19:74:86:a7:66:b4:1a:bf:40:27:21:76:28",
  "description": "Test description.",
  "pattern": "[x509-certificate:issuer = 'CN=WEBMAIL' AND x509-certificate:serial_number = '4c:0b:1d:19:74:86:a7:66:b4:1a:bf:40:27:21:76:28']",
  "indicator_types": [
    "malicious-activity"
```

*SSL-сертификат – это цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное соединение. Аббревиатура SSL означает Secure Sockets Layer – протокол безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером.

X.509 – это стандартный формат для сертификатов открытых ключей, цифровые документы, которые надежно связывают пары криптографических ключей с идентификационными данными. SSL /TLS и HTTPS для аутентифицированного и зашифрованного просмотра веб-страниц. Подписанный и зашифрованный адрес электронной почты через S/MIME протокол

Индикаторы

```
"type": "malware",
"spec_version": "2.1",
"is_family": false,
"id": "malware--2485b844-4efe-4343-84c8-eb33312dd56f",
"created": "2015-05-15T09:12:16.432Z",
"modified": "2015-05-15T09:12:16.432Z",
"name": "MANITSME",
"malware_types": [
    "backdoor",
    "dropper",
    "remote-access-trojan"
],
"description": "This malware will beacon out at random intervals to the remote attacker. The attacker can run programs, execute arbitrary commands, and easily upload and download files."
```

Эта вредоносная программа через случайные промежутки времени посылает сигнал удаленному злоумышленнику. Злоумышленник может запускать программы, выполнять произвольные команды и легко загружать и скачивать файлы.

Инструменты

```
"type": "tool",
  "spec_version": "2.1",
  "id": "tool--ce45f721-af14-4fc0-938c-000c16186418",
  "created": "2015-05-15T09:12:16.432Z",
  "modified": "2015-05-15T09:12:16.432Z",
  "name": "cachedump",
  "tool_types": [
    "credential-exploitation"
  ],
  "description": "This program extracts cached password hashes from a system's registry."
```

*Утилита **cachedump** предназначена для раскрытия информации о кэшированном входе в домен. Работает на 32-битных системах. Инструмент, который демонстрирует, как восстанавливать информацию о записях хеша: имя пользователя и хешированный пароль (называется MSCASH).

CACHEDUMP суффикс имени файла в основном используется для Microsoft Windows System Data Format файлов. CACHEDUMP файлы поддерживаются программными приложениями, доступными для устройств под управлением Windows.

Атака с целью получения учетных записей из кэша домена и различные техники для извлечения хэшей паролей через эксплуатацию пользователя домена.

Domain Cache credential (DCC2)

Microsoft Windows хранит информацию о предыдущей авторизации пользователей локально. Соответственно, эти сведения используются в случае, если сервер авторизации (logon server) окажется недоступным. Эта технология носит название Domain Cache credential (или по другому MSCACHE или MSCASH хэш), которая сортирует хэши паролей пользователей, чтобы вы не смогли выполнить атаки типа pass-the-hash. Для генерации хэшей используется алгоритм MSCACHE, хранящихся локально в реестре операционной системы Windows (по умолчанию, последние 10 хэшей).

Инструменты

```
"type": "tool",
  "spec_version": "2.1",
  "id": "tool--a6dd62d0-9683-48bf-a9cd-61e7eceae57e",
  "created": "2015-05-15T09:12:16.432Z",
  "modified": "2015-05-15T09:12:16.432Z",
  "name": "GETMAIL",
  "tool_types": [
    "information-gathering"
  ],
  "description": "GETMAIL was designed specifically to extract email messages, attachments, and foders from within Microsoft Outlook archive (“PST”) files.

"type": "tool",
  "spec_version": "2.1",
  "id": "tool--806a8f83-4913-4216-bb19-02b48ae25da5",
  "created": "2015-05-15T09:12:16.432Z",
  "modified": "2015-05-15T09:12:16.432Z",
  "name": "MAPIGET",
  "tool_types": [
    "information-gathering"
  ],
  "description": "MAPIGET was designed specifically to steal email that has not yet been archived and still resides on a Microsoft Exchange Server.",
```

Шаблоны атак

```
"type": "attack-pattern",
  "spec_version": "2.1",
  "id": "attack-pattern--3098c57b-d623-4c11-92f4-5905da66658b",
  "created": "2015-05-15T09:12:16.432Z",
  "modified": "2015-05-15T09:12:16.432Z",
  "name": "Initial Compromise",
  "description": "As with most other APT groups, spear phishing is APT1's most commonly used technique. The spear phishing emails contain either a malicious attachment or a hyperlink to a malicious file. The subject line and the text in the email body are usually relevant to the recipient. APT1 also creates webmail accounts using real peoples' names — names that are familiar to the recipient, such as a colleague, a company executive, an IT department employee, or company counsel. The files they use contain malicious executables that install a custom APT1 backdoor that we call WEBC2-TABLE.",
  "external_references": [
    {
      "source_name": "capec",
      "description": "spear phishing",
      "external_id": "CAPEC-163"
    }
  ]
}
```

Шаблоны атак

```
"type": "attack-pattern",
"spec_version": "2.1",
"id": "attack-pattern--1e2c4237-d469-4144-9c0b-9e5c0c513c49",
"created": "2015-05-15T09:12:16.432Z",
"modified": "2015-05-15T09:12:16.432Z",
"name": "Establishing a Foothold",
"description": "APT1 establishes a foothold once email recipients open a malicious file and a backdoor is subsequently installed. In almost every case, APT backdoors initiate outbound connections to the intruder's 'command and control' (C2) server. While APT1 intruders occasionally use publicly available backdoors such as Poison Ivy and Gh0st RAT, the vast majority of the time they use what appear to be their own custom backdoors. APT1's backdoors are in two categories: 'Beachhead Backdoors' and 'Standard Backdoors.' Beachhead Backdoors offer the attacker a toe-hold to perform simple tasks like retrieve files, gather basic system information and trigger the execution of other more significant capabilities such as a standard backdoor. APT1's beachhead backdoors are usually what we call WEBC2 backdoors. WEBC2 backdoors are probably the most well-known kind of APT1 backdoor, and are the reason why some security companies refer to APT1 as the Comment Crew. A WEBC2 backdoor is designed to retrieve a webpage from a C2 server. It expects the webpage to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. WEBC2 backdoors are often packaged with spear phishing emails."}
```

APT1 устанавливает плацдарм, как только получатели электронной почты открывают вредоносный файл - устанавливается бэкдор. Почти в каждом случае бэкдоры APT инициируют исходящие подключения к серверу управления и контроля (C2) злоумышленника. Хотя злоумышленники APT1 иногда используют общедоступные бэкдоры, такие как Poison Ivy и Gh0st RAT, в подавляющем большинстве случаев они используют то, что кажется их собственными бэкдорами.

Бэкдоры APT1 делятся на две категории: «Бэкдоры-плацдармы» и «Стандартные бэкдоры».

- **Бэкдоры-плацдармы** позволяют злоумышленнику выполнять простые задачи, такие как извлечение файлов, сбор базовой системной информации и инициирование выполнения других более важных функций, таких как стандартный бэкдор. Бэкдоры-плацдармы APT1 обычно называются бэкдорами WEBC2.

Бэкдор WEBC2 предназначен для извлечения веб-страницы с сервера C2. Он ожидает, что веб-страница будет содержать специальные теги HTML; бэкдор попытается интерпретировать данные между тегами как команды. Бэкдоры WEBC2 часто поставляются с адресными фишинговыми электронными письмами. После установки злоумышленники APT1 могут указать системам-жертвам загрузить и запустить дополнительное вредоносное программное обеспечение по своему выбору.

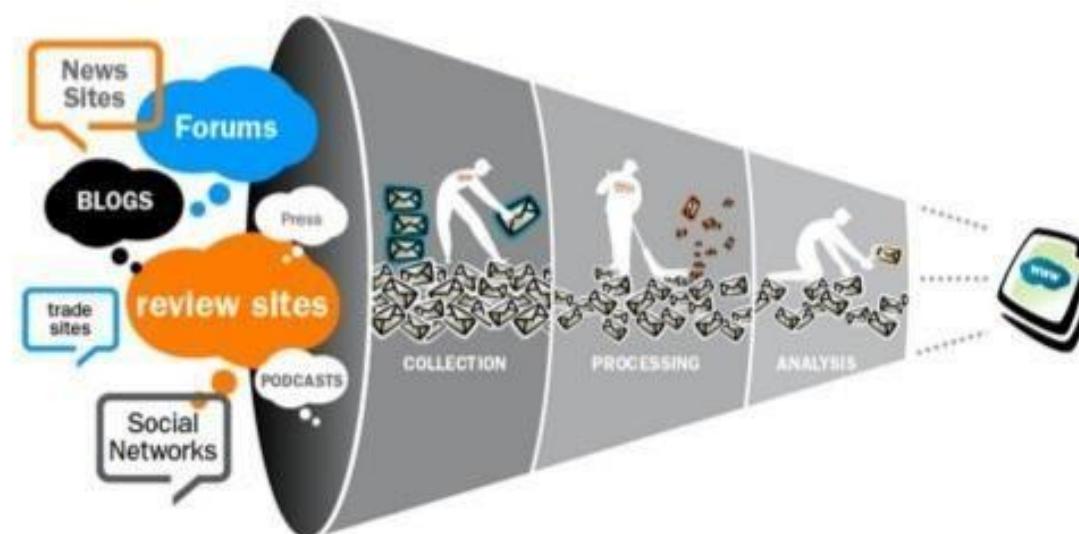
- **Стандартный бэкдор APT1**, не относящийся к WEBC2, обычно взаимодействует с использованием протокола HTTP (чтобы сливатся с законным веб-трафиком) или специального протокола, разработанного самими авторами вредоносного ПО.

Бэкдор BISCUIT (названный так по команде «bdkzt») — наглядный пример набора команд, встроенных в «стандартные» бэкдоры APT1. Некоторые бэкдоры APT пытаются имитировать законный интернет-трафик, отличный от протокола HTTP.

Разведка по открытых источникам

К.т.н., доцент ИКТИБ ЮФУ, Князева М.В.

Open Source Intelligence (OSINT)



ЦЕЛИ И ЗАДАЧИ OSINT

OSINT (Open Source INtelligence) — разведывательная дисциплина и комплекс мероприятий, инструментов и методов для получения и анализа информации из открытых источников. Он применяется в отношении конкретных людей, организаций, а также событий, явлений и целей.

* *OSINT как обособленная дисциплина зародилась в США в 40-х годах прошлого века вместе с учреждением Службы мониторинга зарубежных трансляций. Ее сотрудники записывали и анализировали коротковолновые радиопередачи иностранных государств, после чего полученные данные передавали в виде отчетов военным и разведывательным органам.*

По информации от некоторых представителей ЦРУ и Пентагона, руководство США получало 70–90% данных из открытых источников и только 30–10% — из агентурных.

Сегодня разведка на основе открытых источников используется не только в государственных органах безопасности и обороны, но и в коммерческих компаниях, аналитических агентствах, политических организациях и пр.

ЦЕЛИ И ЗАДАЧИ OSINT

OSINT Landscape v.1 February 2018.

Open Source Intelligence (/OSINv – Open Source Investigation)

COVERTSHORES bellingcat
www.hisutton.com



В IT-индустрии и информационной безопасности OSINT помогает:

- собирать информацию о конкурентах и искать конкурентные преимущества;
- анализировать защищенность объекта, выявлять уязвимые точки системы безопасности;
- находить информационные утечки;
- выявлять возможные угрозы, их источники и направленность;
- анализировать киберпреступления (кражи данных, взломы и т.д.).

ИСТОЧНИКИ ДАННЫХ ДЛЯ OSINT

Open source intelligence подразумевает получение данных из источников в общественном достоянии и/или таких, доступ к которым возможен по запросу. К ним относятся:

- информационные материалы (статьи, новости, заметки) в СМИ; научные исследования, опубликованные в специализированных изданиях; книги, посты и комментарии в социальных сетях;
- форумы, блоги, сайты обмена видео, такие как YouTube.com, вики, Записи Whois о зарегистрированных доменных именах, метаданных и цифровых файлов, даркнет-ресурсы, данные геолокации, IP-адреса;
- информация из переписи;
- документы из открытых государственных и негосударственных архивов;
- публичные коммерческие данные (доход, прибыль, убыток, рост, стоимость акций и т.д.);
- результаты публичных опросов;
- данные со спутников дистанционного зондирования Земли и самолетов аэрофотосъемки;
- полицейские и судебные документы и другие источники.

* Сбор и анализ информации, находящейся в общественном достоянии, не противоречат нормам международного законодательства, а также законам большинства государств, хотя некоторые источники и способы их исследования могут находиться на грани законности.

OSINT в сфере информационной безопасности

С развитием интернета фокус внимания аналитиков сместился в киберпространство как один из главных источников информации. Здесь полезными данными могут являться:

- регистрационные сведения о сертификате или домене сайта;
- открытые персональные данные пользователей (username, адреса электронной почты, номера телефонов);
- пользовательская активность в социальных сетях (посты, комментарии и т.д.);
- пользовательские запросы в поисковых системах;
- HTML-код сайта;
- публичные текстовые, графические, аудио-, видеофайлы и их метаданные (например, дата, время и место создания, использованное устройство);
- геолокационные данные и другие виды информации.

** Ко многим данным можно получить доступ через открытый интернет с помощью ресурсов, индексируемых поисковыми системами. Однако и источники из «глубинной Сети», к которым у обычных пользователей нет доступа из-за необходимости платить за них, тоже попадают под определение open source. Иными словами, OSINT работает со всеми данными, которые не являются конфиденциальными, не составляют коммерческую или государственную тайну.*

Методы OSINT

Все методы и инструменты, используемые в разведке по открытым источникам, можно разделить на две категории.

Пассивные

Позволяют получать общую информацию об объекте. Она собирается вручную или с помощью специальных сервисов и инструментов, упрощающих сбор, систематизацию и анализ данных. Например, программ для парсинга сайтов.

К пассивным методам можно отнести:

- сбор информации (в том числе по фотографиям) из открытых поисковых систем;
- анализ пользовательской активности в социальных сетях и блогах, на форумах, иных виртуальных платформах;
- поиск открытых персональных данных пользователей в социальных сетях, мессенджерах;
- просмотр сохраненных копий сайтов в поисковых системах, интернет-архиве;
- получение геолокационных данных с помощью общедоступных ресурсов вроде Google Maps или Яндекс.Карты.

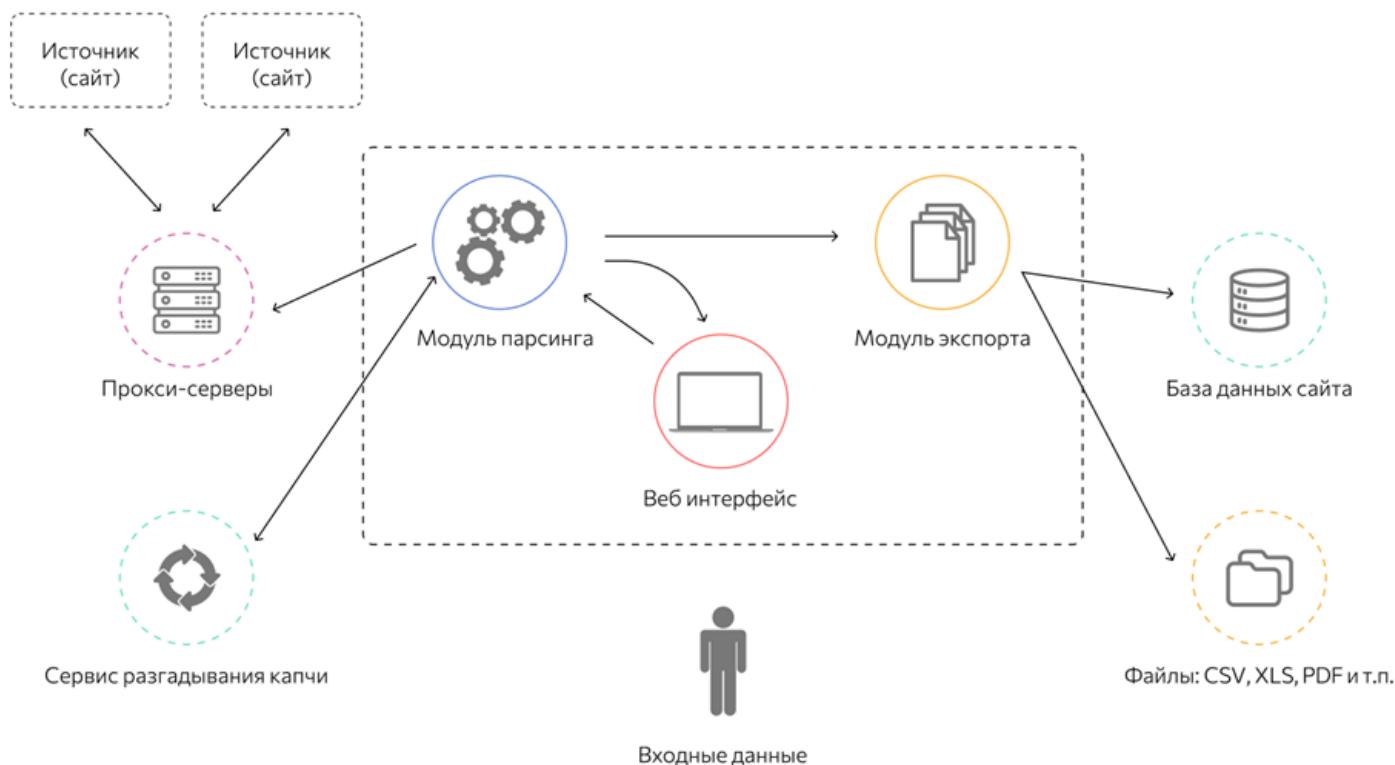
**Парсер — это программа для сбора и систематизации информации, размещенной на различных сайтах. Источником данных может служить текстовое наполнение, HTML-код сайта, заголовки, пункты меню, базы данных и другие элементы. Процесс сбора информации называется парсинг (parsing).*

Процесс представляет собой синтаксический анализ любого набора связанных друг с другом данных.

Парсинг

Процесс представляет собой синтаксический анализ любого набора связанных друг с другом данных. В общем виде **парсинг** выполняется в несколько этапов:

- Сканирование исходного массива информации (HTML-кода, текста, базы данных и т.д.).
- Вычленение семантически значимых единиц по заданным параметрам — например заголовков, ссылок, абзацев, выделенных жирным шрифтом фрагментов, пунктов меню.
- Конвертация полученных данных в формат, удобный для изучения, а также их систематизация в виде таблиц или отчетов для дальнейшего использования.



Парсинг

Объектом парсинга может быть любая грамматически структурированная система: информация, закодированная естественным языком, языком программирования, математическими выражениями и т.д. Например, если исходный массив данных представляет собой HTML-страницу, парсер может вычленить из кода информацию и перевести ее в текст, понятный для человека. Или конвертировать в JSON — формат для приложений и скриптов.

Доступ парсера к сайту возможен:

- через протоколы [HTTP](#), [HTTPS](#) или веб-браузер;
- с использованием бота, имеющего права администратора.

Получение данных парсером — семантический анализ исходного массива информации. Программа разбивает его на отдельные части (лексемы): слова, словосочетания и т.д. Парсер проводит их грамматический анализ, преобразуя линейную структуру текста в древовидную (синтаксическое дерево).

Такая форма упрощает «понимание» информационного массива компьютерной программой и бывает двух типов:

- **дерево зависимостей** — такая структура состоит из компонентов, находящихся в иерархических отношениях друг к другу;
- **дерево составляющих** — в структуре этого типа компоненты находятся в тесной зависимости друг с другом, но без иерархических отношений.

* Распространено мнение, что парсинг сайтов как минимум неэтичен, а в некоторых случаях и незаконен. Действительно, парсеры собирают информацию с чужих веб-ресурсов, баз данных и других источников. Однако в большинстве случаев сведения находятся в открытом доступе, то есть использование программ не нарушает закон.

Методы OSINT

Активные

Такие методы подразумевают непосредственное влияние аналитика на исследуемый объект, использование специализированных средств получения данных или совершение действий, требующих определенных усилий, например:

- сбор данных на закрытых ресурсах, доступ к которым возможен только по подписке;
 - применение специализированных сервисов и программ, которые активно воздействуют на исследуемый объект — например, автоматически регистрируются на сайте;
 - использование сервисов, сканирующих приложения, файлы или сайты на наличие вредоносного кода;
 - создание поддельных веб-ресурсов, каналов в мессенджерах, собирающих данные пользователей, конфиденциальные или секретные сведения.

В логике OSINT пассивные методы, направленные на сбор общей информации из легкодоступных источников, предваряют применение активных способов, предназначенных для сбора конкретных данных об объекте.

Инструменты:

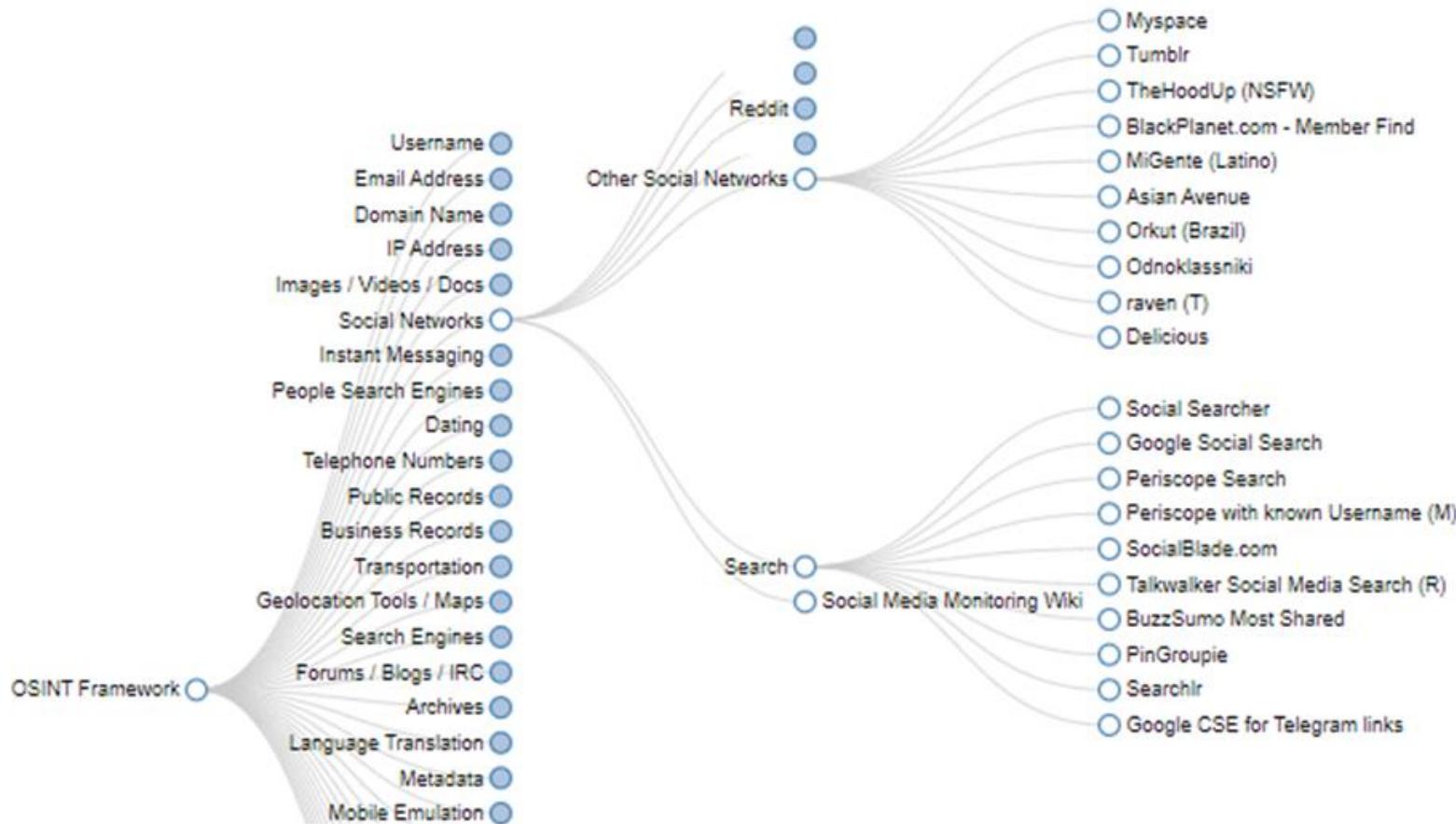
<https://kali.tools/?tag=%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B-%D1%80%D0%B0%D0%B7%D0%B2%D0%B5%D0%B4%D0%BA%D0%B8-%D0%BD%D0%B0-%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B5-%D0%BE%D1%82%D0%BA%D1%80%D1%8B>

Инструменты для OSINT. Примеры

OSINT-фреймворк

Это наиболее полная доступная база открытых источников данных. Они сгруппированы по категориям в интерактивной карте. Кликнув на тот или иной класс, можно выйти на подкласс, а в нем — на конкретный источник информации. OSINT-фреймворк не пропагандирует какую-либо идеологию, это сугубо информационный ресурс, направленный на упрощение поиска в интернете.

<https://osintframework.com/>



Инструменты для OSINT. Примеры

Shodan

Это поисковая система, предназначенная для нахождения подключенных к интернету устройств по IPv4-адресам (роутеры, камеры видеонаблюдения, датчики безопасности и т.д.). Сама система не наносит вреда, но с ее помощью любой желающий при должном старании может найти незащищенное или плохо защищенное устройство.

<https://www.shodan.io/>

The screenshot shows the Shodan search interface. The search bar contains 'webcam'. Below it, there are tabs for 'Explore', 'Downloads', 'Reports', 'Enterprise Access', 'Contact Us', 'My Account', and 'Upgrade'. A 'Like 279' button and a 'Download Results' button are also present. On the left, there's a 'TOP COUNTRIES' section with a world map and a table of top countries: United States (807), Korea, Republic of (373), Germany (271), Italy (180), and Russian Federat... (137). To the right, the search results for '99.192.179.104' are displayed, showing it's a Mojohost server from the United States, Franklin, added on 2016-08-22. It lists various details like HTTP headers and XML content. Another result for '99.192.129.92' is partially visible at the bottom.

COUNTRY	RESULTS
United States	807
Korea, Republic of	373
Germany	271
Italy	180
Russian Federat...	137

SERVICE	RESULTS
HTTP (8080)	1,501
HTTP	343
HTTPS	316
AndroMouse	98
Insteon Hub	92

Инструменты для OSINT. Примеры

Metagoofil

Это метапоисковая система, которая использует другие поисковики для нахождения и извлечения находящихся в открытом доступе файлов PDF, Word, Powerpoint и Excel. С ее помощью можно парсить техническую документацию, клиентские базы данных, справочники, каталоги и прочие полезные источники.

<https://www.kali.org/tools/metagoofil/>

Инструменты для OSINT. Примеры

Maltego – графический анализ данных

Инструмент OSINT предназначенный для поиска данных о людях, компаниях. Работает на платформах Windows, Linux и MacOS. Ключевая особенность программы в том, что она определяет соотношения между данными, создает графическое отображение данных. На графиках и диаграммах можно просматривать до 1млн объектов. Maltego автоматизирует поиск, что позволяет пользователям одним кликом выполнить несколько запросов.

Основное внимание в приложении уделяется анализу реальных отношений (социальные сети, OSINT API, самостоятельных узлов частных данных и компьютерных сетей) между людьми, группами, веб-страницами, доменами, сетями, интернет-инфраструктурой и принадлежностью социальных сетей.

Среди его источников данных — записи DNS, записи whois, поисковые системы, службы социальных сетей, различные API и метаданные.

Maltego — это программа, которая может быть использована для выявления отношений и реальных связей между:

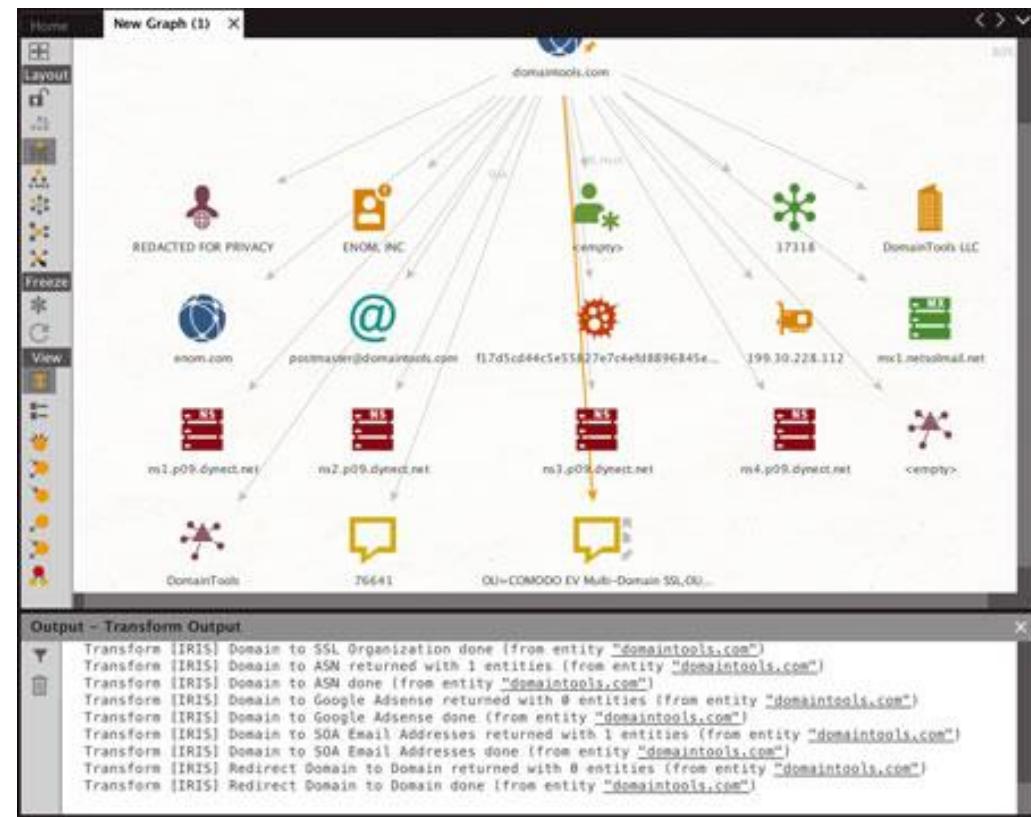
- Людьми, Группами людей (социальные сети), Компаниями, Организациями, Веб-сайтами
- Интернет инфраструктурами, такими как:

Доменами

DNS именами

Сетевыми блоками

IP адресами



Инструменты для OSINT. Примеры

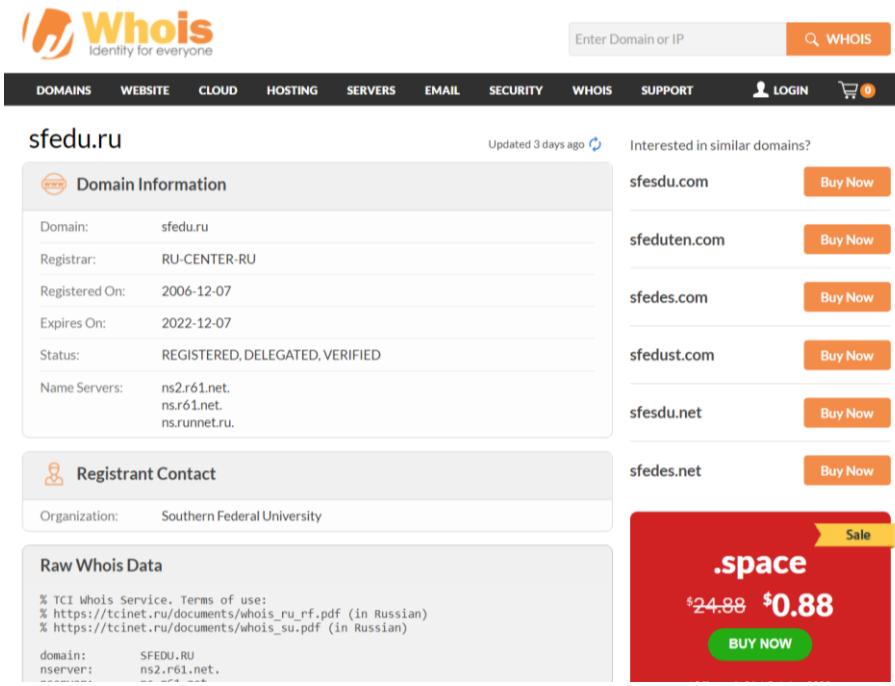
DNS (англ. Domain Name System «система доменных имён») — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене (SRV-запись).

WHOIS (от англ. who is — «кто это?») — сетевой протокол прикладного уровня, базирующийся на протоколе TCP (порт 43). Основное применение — получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем.

Например, запрос о доменном имени:

\$> whois wikipedia.org

<https://www.whois.com/whois/wikipedia.org>



Whois search results for sfedu.ru:

Domain Information	
Domain:	sfedu.ru
Registrar:	RU-CENTER-RU
Registered On:	2006-12-07
Expires On:	2022-12-07
Status:	REGISTERED, DELEGATED, VERIFIED
Name Servers:	ns2.r61.net. ns.r61.net. ns.runnet.ru.

Registrant Contact:

Organization:	Southern Federal University
---------------	-----------------------------

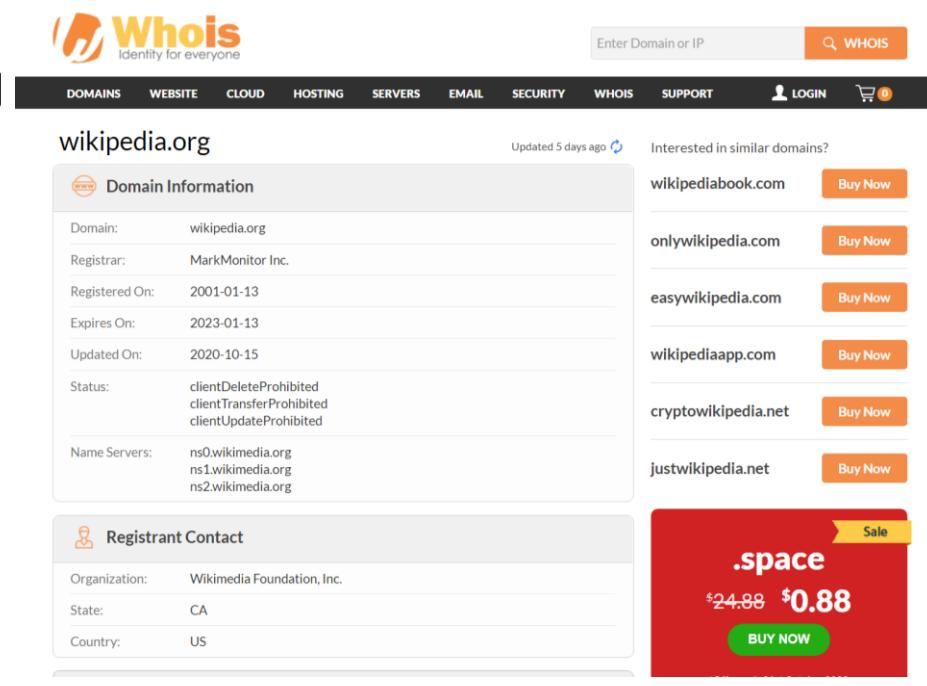
Raw Whois Data:

```
% TCI Whois Service. Terms of use:  
% https://tcinet.ru/documents/whois_ru_rf.pdf (in Russian)  
% https://tcinet.ru/documents/whois_su.pdf (in Russian)
```

domain: SFEDU.RU
nsrserver: ns2.r61.net.

WHOIS API Call:

```
curl -X GET "https://www.whois.com/whois/sfedu.ru"
```



Whois search results for wikipedia.org:

Domain Information	
Domain:	wikipedia.org
Registrar:	MarkMonitor Inc.
Registered On:	2001-01-13
Expires On:	2023-01-13
Updated On:	2020-10-15
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns0.wikimedia.org ns1.wikimedia.org ns2.wikimedia.org

Registrant Contact:

Organization:	Wikimedia Foundation, Inc.
State:	CA
Country:	US

WHOIS API Call:

```
curl -X GET "https://www.whois.com/whois/wikipedia.org"
```

Инструменты для OSINT. Примеры

API (аббр. от англ. Application Programming Interface) — описание способов взаимодействия одной компьютерной программы с другими. Обычно входит в описание какого-либо интернет-протокола (например, SCIM), программного каркаса (фреймворка) или стандарта вызовов функций операционной системы. Часто реализуется отдельной программной библиотекой или сервисом операционной системы. Используется программистами при написании всевозможных приложений.

Web API

Используется в веб-разработке — содержит, как правило, определённый набор HTTP-запросов, а также определение структуры HTTP-ответов, для выражения которых используют XML- или JSON-формат.

Методы HTTP определяют действие, которое необходимо выполнить с ресурсом. Значение HTTP-методов описывается спецификацией протокола. Спецификация протокола HTTP не ограничивает количество различных методов, которые могут быть использованы. Однако для поддержки совместимости с широким спектром приложений используются только некоторые из наиболее стандартных методов.

Ниже перечислены некоторые методы HTTP, которые можно использовать в вызовах API.

GET – для получения (чтения) данных (например, списка пользователей).

POST – для создания новых данных.

PUT / PATCH – для обновления данных.

DELETE – для удаления данных.

OPTIONS – чтобы получить полное описание методов API, доступных на сервисе.

Заголовок содержит метаданные, позволяющие клиенту передавать уточняющую и служебную информацию о HTTP-запросе, такую как сведения о кодировке, параметры авторизации и т. д.

Информация, которую вы хотите передать по сети, передается в теле. Тело является необязательным и может быть оставлено пустым (в зависимости от методов HTTP и заголовков).

HTTP-ответ — это данные, которые возвращаются с сервера API. Помимо данных в теле, заголовок ответа содержит HTTP-код состояния ответа сервера. Например, в заголовке ответа можно получить следующие коды состояния:

200 – Успех;

400 – Плохой запрос;

401 – Несанкционированно.

OSINT и социальные сети

Аналитика социальных сетей (**SOCMINT**) — это подразделение аналитики с открытым исходным кодом (OSINT), которое относится к информации, собранной с веб-сайтов социальных сетей. Данные, доступные на сайтах социальных сетей, могут быть общедоступными (например, общедоступные сообщения в ВКонтакте) или частными.

Данные, доступные на сайтах социальных сетей, можно разделить на две категории:

Исходный контент, размещенный пользователем, например текстовый контент или загруженное изображение/видео.

Метаданные, связанные с исходным контентом — метаданные мультимедийных файлов, дата/время и информация о географическом местоположении, связанные с размещенным контентом

OSINT и социальные сети

Используя документацию к API VK , составим запросы для получения списка фотографий по географической информации и времени. Здесь используемые переменные:

location_latitude — географическая широта;

location_longitude — географическая долгота;

distance — радиус поиска;

timestamp — начальная граница интервала времени;

date_increment — количество секунд от начальной до конечной границы интервала времени;

access_token — токен разработчика.

Vkontakte API Request:

```
url = "https://api.vk.com/method/photos.search?"  
+ "lat=" + location_latitude  
+ "&long=" + location_longitude  
+ "&count=" + 100  
+ "&radius=" + distance  
+ "&start_time=" + timestamp  
+ "&end_time=" + (timestamp + date_increment)
```

OSINT и социальные сети

API ВКонтакте представляет собой набор готовых методов для получения интересующей нас информации из базы данных ВКонтакте.

Всю информацию про API VK можно найти по ссылке: <https://dev.vk.com>

На данной странице содержится исчерпывающее описание всех возможных манипуляций, которые можно осуществить посредством API.

Данный интерфейс позволит нам получить интересующую нас информацию из базы данных VK с помощью http-запросов. Мы будем посылать http-запросы согласно документации vk-API и получать ответы в виде JSON объектов.

Чтобы обратиться к методу API ВКонтакте нужно выполнить POST или GET запрос определенного вида:
«https://api.vk.com/method/METHOD?PARAMS&access_token=TOKEN&v=V»

The screenshot shows the VK API documentation interface. At the top, there's a navigation bar with links for 'для разработчиков' (For Developers), 'Документация' (Documentation), 'API' (which is underlined), 'Создать приложение' (Create Application), a search bar with placeholder 'Поиск' (Search), and a 'Войти' (Log In) button. The main content area has a sidebar on the left listing various API endpoints like Account, Ads, AppWidgets, etc. The central column is titled 'API' and contains sections for 'Ключ доступа' (Access Key), 'Права доступа' (Access Rights), 'Формат запросов' (Request Format), 'Коды ошибок' (Error Codes), 'JSON-схема' (JSON Schema), 'Объекты' (Objects), 'Состояние API' (API Status), and 'Методы API' (API Methods). A sidebar on the right is titled 'На этой странице' (On this page) and lists links to 'Ключ доступа', 'Права доступа', 'Формат запросов', 'Коды ошибок', 'JSON-схема', 'Объекты', 'Состояние API', and 'Методы API'. At the bottom, there are footer links for '© 2022 ВКонтакте', 'Поддержка', 'Правила', and 'vk.com/dev'.

OSINT и социальные сети

Чтобы обратиться к методу API ВКонтакте нужно выполнить POST или GET запрос определенного вида:
«https://api.vk.com/method/METHOD?PARAMS&access_token=TOKEN&v=V»

Запрос состоит из нескольких частей, в которых присутствуют обязательные части и необязательные.

1. METHOD – обязательная часть запроса, в которой указывается название метода API, к которому мы хотим обратиться, имя метода чувствительно к регистру.
2. PARAMS – необязательная часть запроса, в данной части указываются параметры запроса которые имеют вид последовательности пар (ключ - значение), разделенных амперсандом. Список параметров указывается на странице с описанием метода.
3. TOKEN – обязательная часть запроса, является ключом доступа.

Для начала работы с API ВКонтакте нам понадобится токен. В запросе токен указывается в паре с access_token= «TOKEN».

Сам по себе токен представляет собой строку из латинских букв и цифр и может соответствоватьциальному пользователю, сообществу или приложению.

Для получения ключа доступа используется открытый протокол OAuth 2.0. При этом пользователь не передает логин и пароль приложения, поэтому его аккаунт не может быть скомпрометирован.

4. V – обязательная часть, отображает используемую версию API. Информацию об актуальной версии API всегда можно найти на странице информации об API.

* Параметры в запрос могут передаваться как методом GET, так и POST. Если планируется передавать большие данные (больше 2 килобайт), следует использовать запрос POST и формат FormData.

** Так же существуют общие параметры, которые могут применяться независимо от используемого метода. Например, такой параметр как «Lang» отвечает за язык, в котором нам вернется JSON ответ. На данный момент API поддерживает восемь языков в числе которых: русский, украинский, белорусский, английский, испанский, финский, немецкий, итальянский. По умолчанию если данный параметр не указан будет использован английский язык.

*** У API ВКонтакте существуют ограничения ко всем методам за редким исключением (методы secure и ads) с ключом доступа пользователя можно обращаться не чаще 3 раз в секунду. Для ключа доступа сообщества ограничение составляет 20 запросов в секунду. А для приложения, которому требуется большой количество запросов, существует метод execute. Он позволяет совершать 25 обращений к разным методам в рамках одного запроса.

Инструменты для OSINT. Google Dorks.

Google Dorks или **Google Hacking** — техника, используемая СМИ, следственными органами, инженерами по безопасности и любыми пользователями для создания запросов в различных поисковых системах для обнаружения скрытой информации и уязвимостях, которые можно обнаружить на общедоступных серверах. Это метод, в котором обычные запросы на поиск веб-сайтов используются в полную меру для определения информации, скрытой на поверхности.

* Google Dork или Google Dork Queries (GDQ) — это набор запросов для выявления грубейших дыр в безопасности ресурсов.

Операторы Google:

site — искать по конкретному сайту;

inurl – указать на то, что искомые слова должны быть частью адреса страницы / сайта;

intitle — оператор поиска в заголовке самой страницы;

ext или *filetype* — поиск файлов конкретного типа по расширению.

— оператор OR он же вертикальный слеш (логическое или) указывает, что нужно отобразить результаты, содержащие хотя бы одно из слов, перечисленных в запросе.

«» — оператор кавычки указывает на поиск точного соответствия.

— — оператор минус используется для исключения из выдачи результатов с указанными после минуса словами.

* — оператор звездочка, или астериск используют в качестве маски и означает «что угодно».



Google Dorks

Онлайн-сервис Exploit-DB — это некоммерческий проект Offensive Security, данная компания занимается обучением в области информационной безопасности, а также предоставляет услуги пентеста.

База данных Exploit-DB насчитывает огромное количество дорков и уязвимостей.

*Для поиска дорков зайдите на сайт exploit-db.com и перейдите на вкладку «Google Hacking Database».

<https://www.exploit-db.com/google-hacking-database>

The screenshot shows the Exploit-DB website interface. On the left, there's a sidebar with icons for EXPLOIT DATABASE, EXPLOITS, GHDB (which is highlighted), PAPERS, SHELLCODES, SEARCH EDB, and SEARCHSPLOIT MANUAL. The main content area has a dark blue header with the text 'HACKING DATABASE'. Below it, the title 'Hacking Database' is displayed. To the right is a search bar with 'Quick Search' and 'Filters' buttons. A 'Reset All' button is also visible. The main content area lists several Google Dork queries with their corresponding categories and authors:

Dork	Category	Author
intext:"index of" ".sql"	Files Containing Juicy Info	Gopalsamy Rajendran
intitle:"index of" inurl:superadmin	Files Containing Juicy Info	Mahedi Hassan
intitle:"WAMPSERVER Homepage"	Files Containing Juicy Info	HackerFrenzy
inurl: json beautifier online	Files Containing Juicy Info	Nyein Chan Aung
intitle:"IIS Windows Server"	Files Containing Juicy Info	HackerFrenzy
intitle:"index of" inurl:SUID	Files Containing Juicy Info	Mahedi Hassan

Google Dork Description: inurl:"admin/default.aspx"

Выдает список адресов страниц
автентификации админов

The screenshot shows a search result for the Google Dork "inurl:admin/default.aspx" on the Exploit Database. The search bar at the top contains the query. Below it, the search results are displayed in two columns. The left column contains details for a specific entry: GHDB-ID: 8021, Author: PAYAL YEDHU, and Published: 2022-08-17. The right column contains the Google Dork Description and a link to the Google search results. At the bottom of the page, there is a code block with comments explaining the dork. The footer of the website includes links for Downloads, Certifications, Training, and Professional Services, along with information about Kali Linux, OSCP, and various penetration testing courses.

EXPLOIT DATABASE

inurl:"admin/default.aspx"

GHDB-ID: 8021 **Author:** PAYAL YEDHU

Published: 2022-08-17

Google Dork Description:
inurl:"admin/default.aspx"

Google Search: inurl:"admin/default.aspx"

```
# Google Dork: inurl:"admin/default.aspx"
# Category: Pages Containing Login Portals
# Date: 07/08/2022
# Exploit Author: Payal Yedhu
```

Downloads Certifications Training Professional Services

Kali Linux OSCP Penetration Testing with Kali Linux (PWK) (PEN-200)
All new for 2020

Penetration Testing

Google Dork Description: inurl:"admin/default.aspx"

Результат поиска и процесса аутентификации

readydesk.com/rd9/hd/admin/admin.aspx

The screenshot shows a web browser window with the URL `readydesk.com/rd9/hd/admin/admin.aspx`. On the left, there is a sidebar menu with various administrative options like Home, Quick Start, User Manual, Database, Settings, Technicians, Groups, Companies, Customers, Support Contracts, Active Directory, Single Sign-on, Customization, Automation, Workflow, Email Management, Ticket Management, Attachments, Knowledge Base, News, Surveys, Site Traffic, Live Chat, Remote Desktop, Call Management, Asset Management, Network Inventory, Multi-language, Billing, Service Levels, Scheduling, Time Tracking, Reports & Charts, Web Services API, and Whiteboard. At the bottom of the sidebar, there is a Log Off link. The main content area features a large central dialog box with a warning icon and the text "Смените пароль" (Change password). Below the dialog, a message states: "В результате утечки данных на одном из сайтов или в одном из приложений ваш пароль оказался раскрыт. Рекомендуем сменить пароль для следующего ресурса: www.readydesk.com." At the bottom of the dialog, there is an "OK" button and an "Email Status" link. Below the dialog, there are several summary cards: "Status - Current (0 tickets)" showing counts for 1st Callback, Awaiting Response, Customer Approved, Open, Pending, and Technician Responded; "Category - Current (0 tickets)" showing counts for Category 1, Category 2, Expense, and Labor; "Sub-Category - Current (0 tickets)" showing counts for Domain ID Configuration, 311, 32, 322, donald duck, Hardware, Remove account, Smartboard, and test subcat; and three empty cards for "Source - Current (0 tickets)", "Assigned Groups - Current (0 tickets)", and "Assigned Technicians - Current (0 tickets)".

Google Dork Description: inurl:"admin/default.aspx"«

Результат успешной аутентификации

The screenshot shows the ReadyDesk Administration Console interface. On the left is a navigation sidebar with various menu items like Home, Quick Start, User Manual, Database, Settings, Technicians, Groups, Companies, Customers, Support Contracts, Active Directory, Single Sign-on, Customization, Automation, Workflow, Email Management, Ticket Management, Attachments, Knowledge Base, News, Surveys, Site Traffic, Live Chat, Remote Desktop, Call Management, Asset Management, Network Inventory, Multi-language, Billing, Service Levels, Scheduling, Time Tracking, Reports & Charts, Web Services API, Whiteboard, and Log Off. The main area features the ReadyDesk logo and a welcome message: "Welcome to the ReadyDesk Administration Console". A central box displays system information: Version: 9.5, Build: 9.5.0, Licensed To: jpn21, Technician Licenses: 1 (with a link to Add Licenses), Technicians Logged In: 1, Server Date/Time: 23.10.2022 9:37:39, Open Tickets: 0, and Email Status: rd9@readydesk.com: 110. Below this are four cards: Status - Current (0 tickets) showing ticket counts for various stages (1st Callback, Awaiting Response, Customer Approved, Customer Responded, Open, Pending, Technician Responded); Category - Current (0 tickets) showing ticket counts for categories (Category 1, Category 2, Expense, Labor); Sub-Category - Current (0 tickets) showing ticket counts for sub-categories (Domain ID Configuration, donald duck, Hardware, Remove account, Smartboard, test subcat); and Source - Current (0 tickets), Assigned Groups - Current (0 tickets), and Assigned Technicians - Current (0 tickets).

Google Dork Description:

intext:"index of" ".sql"

SQL Dump – файл, включающий в себя содержимое памяти компьютера или базы данных. В нашем случае это файл с расширением .sql. Он содержит особые данные, благодаря которым можно легко воссоздать копию БД.

The screenshot shows a web browser displaying the Exploit Database (GHDB) at the URL exploit-db.com/ghdb/8030. The page title is "EXPLOIT DATABASE". On the left, there is a vertical sidebar with various orange icons representing different tools and services. The main content area displays a search result for the Google Dork "intext:index of ".sql)".

GHDB-ID: 8030 **Author:** GOPALSAMY RAJENDRAN

Published: 2022-09-19

Google Dork Description:
intext:"index of" ".sql"

Google Search: intext:"index of" ".sql"

Google Dork: intext:"index of" ".sql"
Files Containing Juicy Info
Date:19/09/2022
Exploit Author: Gopalsamy Rajendran

Downloads Certifications Training Professional Services

Kali Linux OSCP Penetration Testing with Kali Linux (PWK) (PEN-200)
All new for 2020 Penetration Testing

Offensive Security Wireless Attacks (WEA) (PEN-210)

Advanced Attack Simulation

Google Dork Description: для поиска IP-камер, медиасерверов и веб-админок

С помощью продвинутых запросов к Google можно найти массу сетевых устройств с управлением через веб-интерфейс.

Наиболее часто для этого используются сценарии CGI, поэтому файл main.cgi — перспективная цель. Однако встретиться он может где угодно, поэтому запрос лучше уточнить.

Например, добавив к нему типовой вызов ?next_file.

В итоге получим дork вида:

inurl:"img/main.cgi?next_file"

The screenshot shows a Google search results page with the query "inurl:'img/main.cgi?next_file'" entered in the search bar. The results are filtered under the "Все" (All) tab. There are 43 results in total, displayed over 0.22 seconds.

Result 1: <http://99.159.106.81> > img ▾ [Перевести эту страницу](#)
Live Video - Network Camera
Home | Administration. 1. H264, 2. H264, 3. H264, 4. MJPEG. QuickTime, FlashPlayer. D/N Mode. Preset Points. Click here to install or upgrade the H.264 ...

Result 2: http://cam_snekkevik.grygier.net > ... ▾ [Перевести эту страницу](#)
Network Camera - Live Video
Home | Administration. Preset Points. None, Aussicht - view, Links - left, Rechts - right, Aussicht2 - view. Video Movement. Video for other Platform/OS.

Result 3:  Картинки по запросу inurl:'img/main.cgi?next_file'
[Показать все →](#)

<http://61.92.70.65> > img ▾ [Перевести эту страницу](#)
Live Video - Network Camera
undefined. Home | Administration. 1. MJPEG, 2. MPEG-4, 3. H264. Output. Preset Points.

Google Dork Description: для поиска уязвимостей

Hadoop (система обработки Big Data) — один из простейших способов скомпрометировать тера- и даже петабайты данных (настройки по умолчанию). Эта платформа с открытым исходным кодом содержит известные заголовки, номера портов и служебных страниц, по которым просто отыскать управляемые ей ноды.

intitle:"Namenode information" AND inurl:"/dfshealth.html"

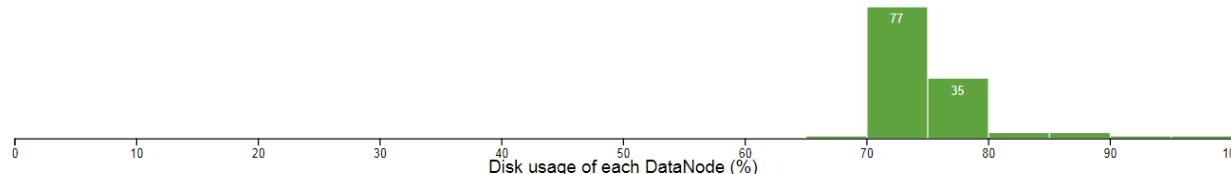
Таким запросом с конкатенацией мы получаем поисковую выдачу со списком уязвимых систем на базе Hadoop. Можно прямо из браузера обратиться к файловой системе HDFS и скачать файлы.

A screenshot of the Hadoop Web UI. At the top, there's a navigation bar with tabs: Hadoop, Overview, Datanodes (which is highlighted in blue), Datanode Volume Failures, Snapshot, Startup Progress, and Utilities. Below the navigation bar, the main content area has a title 'Datanode Information'. Underneath the title, there's a legend with five status indicators: 'In service' (green checkmark), 'Down' (red exclamation mark), 'Decommissioned' (orange circle), 'Decommissioned & dead' (blue circle), and 'In Maintenance & dead' (orange wrench).

Datanode Information

✓ In service ⚠ Down ⚡ Decommissioned ⚡ Decommissioned & dead 🔧 In Maintenance & dead

Datanode usage histogram



In operation

Show entries

Search:

Node	Last contact	Capacity	Blocks	Block pool used	Version
✓ cabinet-0-0-0.t2.ucsd.edu (169.228.131.254:50010)	Sun Oct 23 17:27:02 +0300 2022	21.49 TB	892662	16.11 TB (75%)	2.6.0-cdh5.12.1
✓ cabinet-0-0-10.t2.ucsd.edu (169.228.131.244:50010)	Sun Oct 23 17:27:00 +0300 2022	21.49 TB	854103	15.98 TB (74.36%)	2.6.0-cdh5.12.1
✓ cabinet-0-0-11.t2.ucsd.edu (169.228.131.243:50010)	Sun Oct 23 17:27:02 +0300 2022	21.49 TB	821807	15.25 TB (70.98%)	2.6.0-cdh5.12.1



Матрица ATT&CK

Язык описания угроз MITRE

attack.mitre.org

High Level Models
(Lockheed Martin Kill Chain®,
Microsoft STRIDE)

Mid-level Model (MITRE ATT&CK)

Low Level Concepts
(Exploit & Vulnerability
databases & models)

К.т.н., доцент ИКТИБ ЮФУ
Князева Маргарита Владимировна

Проекты MITRE

CVE (Common Vulnerabilities and Exposures) – язык и формат описания уязвимостей;

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), attack.mitre.org — это структурированный список известных техник, приемов и тактик злоумышленников, представленный в виде таблиц;

Structured Threat Information Expression (STIX) — это язык и формат сериализации, используемый для обмена информацией о киберугрозах (CTI — Cyber Threat Intelligence) между системами информационной безопасности;

CAR (Cyber Analytics Repository) — база знаний, разработанная на основе модели ATT&CK. Она может быть представлена в виде псевдокода, и команды защитников могут использовать ее при создании логики детектирования в системах защиты;

SHIELD Active Defense — база знаний по активной защите, которая систематизирует методы безопасности и дополняет меры снижения рисков, представленные в ATT&CK;

AEP (ATT&CK Emulation Plans) — это способы моделирования поведения злоумышленника на основе определенного набора TTP (Tactics, Techniques, and Procedures) по ATT&CK.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

MITRE представил матрицу **ATT&CK** в 2013 году как способ описания и категоризации поведения злоумышленников (составления паттернов поведения Cyber Kill Chain) на основе реальных наблюдений над APT-атаками. Помимо нее была создана дополнительная база знаний **PRE-ATT&CK**, описывающая подготовку к атаке; и **ATT&CK** для мобильных устройств.

Наборы TTP (техники, тактики и процедуры):

тактика — как злоумышленник действует на разных этапах своей операции, какая цель или задача злоумышленника на определенным шаге, например: TA0002 Execution — это когда злоумышленник пытается запустить свой вредоносный код.

техника — как злоумышленник достигает цели или поставленной задачи, какие использует инструменты, технологии, код, эксплоиты, утилиты и так далее. Пример: T1059.001 PowerShell — использование PowerShell при атаке;

процедура — как эта техника выполняется и для чего. Например: вредоносная программа, используя PowerShell, скачивает пейлоад, который, в свою очередь, загружает Cobalt Strike для попытки запуска на удаленных хостах.

**PowerShell — расширяемое средство автоматизации от Microsoft с открытым исходным кодом, состоящее из оболочки с интерфейсом командной строки и сопутствующего языка сценариев.*

PowerShell также предоставляет механизм встраивания, благодаря которому исполняемые компоненты PowerShell могут быть встроены в другие приложения. Эти приложения затем могут использовать функциональность PowerShell для реализации различных операций, включая предоставляемые через графический интерфейс.

MITRE разбил ATT&CK на несколько сводных матриц:

Enterprise — TTP, используемые при атаках на организации;

Mobile — TTP, связанные с переносными устройствами;

ICS — Industrial Control Systems, TTP для индустриальных систем.

MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge — «тактики, техники и общеизвестные факты о злоумышленниках»)

Модель ATT&CK занимает среднее положение в иерархии:

High Level Models
(Lockheed Martin Kill Chain®,
Microsoft STRIDE)

Mid-level Model (MITRE ATT&CK)

Low Level Concepts
(Exploit & Vulnerability
databases & models)

APT-атаки и Kill Chain

APT (англ. Advanced Persistent Threat — «развитая устойчивая угроза»; также целевая кибератака) - противник, обладающий современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения (например, информационных, физических и обманных).

Эти цели обычно включают установление и расширение своего присутствия внутри информационно-технологической инфраструктуры целевой организации для осуществления намерений извлечения информации, срыва или создания помех критическим аспектам выполняемой задачи, программы или службы; либо для того, чтобы занять позицию, позволяющую осуществить эти намерения в будущем. APT, как «развитая устойчивая угроза»: добивается своих целей неоднократно в течение длительного времени; адаптируется к усилиям защищающихся оказать угрозе сопротивление; имеет установку сохранить уровень проникновения в целевой инфраструктуре, требуемый для осуществления намерений.

Kill Chain, то есть «цепочка убийства», — модель, определяющая последовательность действий, ведущих нарушителя к цели.

Она состоит из ряда обычно последовательных этапов:

reconnaissance — разведка;

weaponization — подготовка к атаке, определение инструментария и delivery — доставка;

exploitation — эксплуатация арсенала;

installation — установка;

command & control (C2) — управление через командные серверы;

lateral movement — горизонтальное перемещение, распространение внутри сети;

objectives — целевое воздействие.

АРТ-атаки и их особенности

- Это атаки, направленные в отношении конкретных коммерческих организаций, отраслей производства или государственных ведомств.
- Объектами атаки являются весьма ограниченные какими-либо рамками или целями конкретные информационные системы.
- Эти атаки не носят массовый характер и готовятся достаточно длительный период.
- Вредоносное ПО, если оно используется при реализации атаки, специально разрабатывается для конкретной атаки, чтобы штатные средства защиты, достаточно хорошо изученные злоумышленниками, не смогли обнаружить ее реализацию.
- Для реализации атаки могут использоваться уязвимости нулевого дня.
- Как правило, целевые атаки используются для кражи информации, которую легко монетизировать, либо для нарушения доступности к критически важной информации.
- При осуществлении целевой атаки используются те же механизмы взлома, что и при массовых атаках, в частности фишинг. Отличие составляет подготовка атаки с целью предотвращения возможности ее детектирования средствами защиты. Именно применительно к целевым атакам фишинг становится очень актуальной угрозой, поскольку атака в этом случае осуществляется не на абстрактные, а на конкретные физические лица, что может быть учтено методами социальной инженерии.
- После обнаружения и идентификации целевой атаки, уже по итогам ее осуществления, об угрозе этой атаки становится известно, она переходит в категорию «массовых» - может массово использоваться злоумышленниками. При этом, как идентифицированная, угроза этой атаки уже может детектироваться средствами защиты, одной из задач которых является обеспечение минимальной продолжительности перехода угрозы атаки из категории целевых в массовые.

АРТ-атаки и их особенности

ТАРГЕТИРОВАННАЯ АТАКА



КТО ЗЛОУМЫШЛЕННИК?

- Энтузиасты
- «Обиженные» сотрудники
- Организованные преступные группировки

НЕТАРГЕТИРОВАННАЯ АТАКА



КТО ЗЛОУМЫШЛЕННИК?

- Любители
- «Скрипт-школьники»

ДОСТИЖЕНИЕ ЦЕЛЕЙ

- Хищение ключевой информации
- Изменение данных
- Манипуляции с бизнес процессами
- Сокрытие следов
- Точка возврата



ПОДГОТОВКА

- Выявление цели
- Сбор информации
- Разработка стратегии
- Создание стенда
- Разработка инструментов



Фазы целевой атаки

РАСПРОСТРАНЕНИЕ

- Закрепление
- Распространение
- Обновление
- Поиск ключевой информации и методов достижения целей



ПРОНИКНОВЕНИЕ

- Техники обхода стандартных средств защиты
- Эксплуатация уязвимостей
- Социальная инженерия
- Комбинированные техники
- Инвентаризация сети



Подготовка



Получение информации

Социальная инженерия

Фишинговые ссылки

Проникновение



– Получены данные

Целевой фишинг

Эксплойты

Инсайдеры

Уязвимости нулевого дня

Распространение



– Тиражирование в системе

RAT

Бэкдоры

Самоуничтожение

Реализация цели



Кейлоггеры

Шпионы

Перехват

СРЕДСТВО РЕАЛИЗАЦИИ

РЕЗУЛЬТАТ РЕАЛИЗАЦИИ

Извлечение конфиденциальных данных жертвы

– Подготовка

Внедрение средства удаленного администрирования

– Начало реализации
– Не завершена

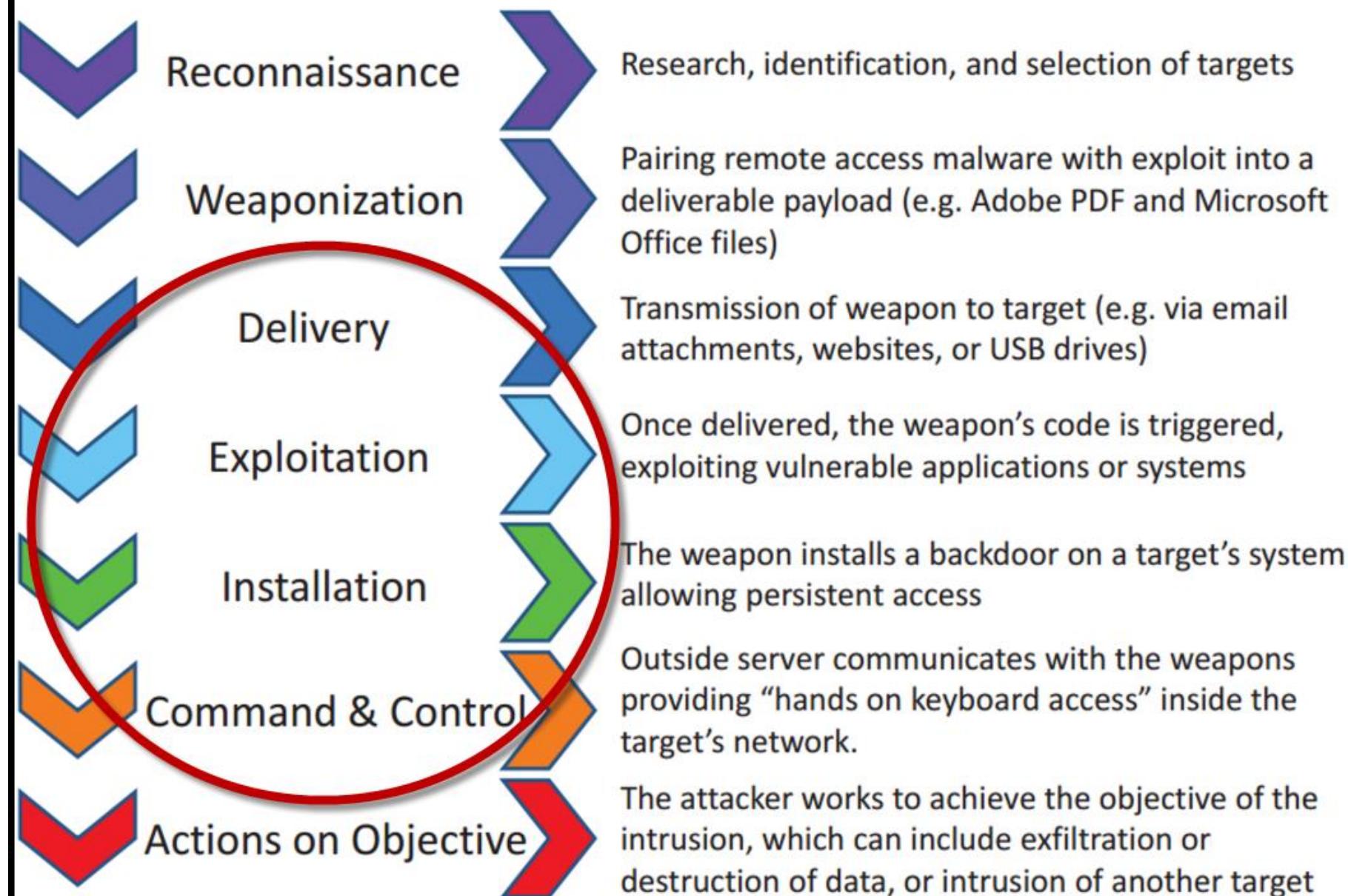
Заражение и получение доступа к управлению данными

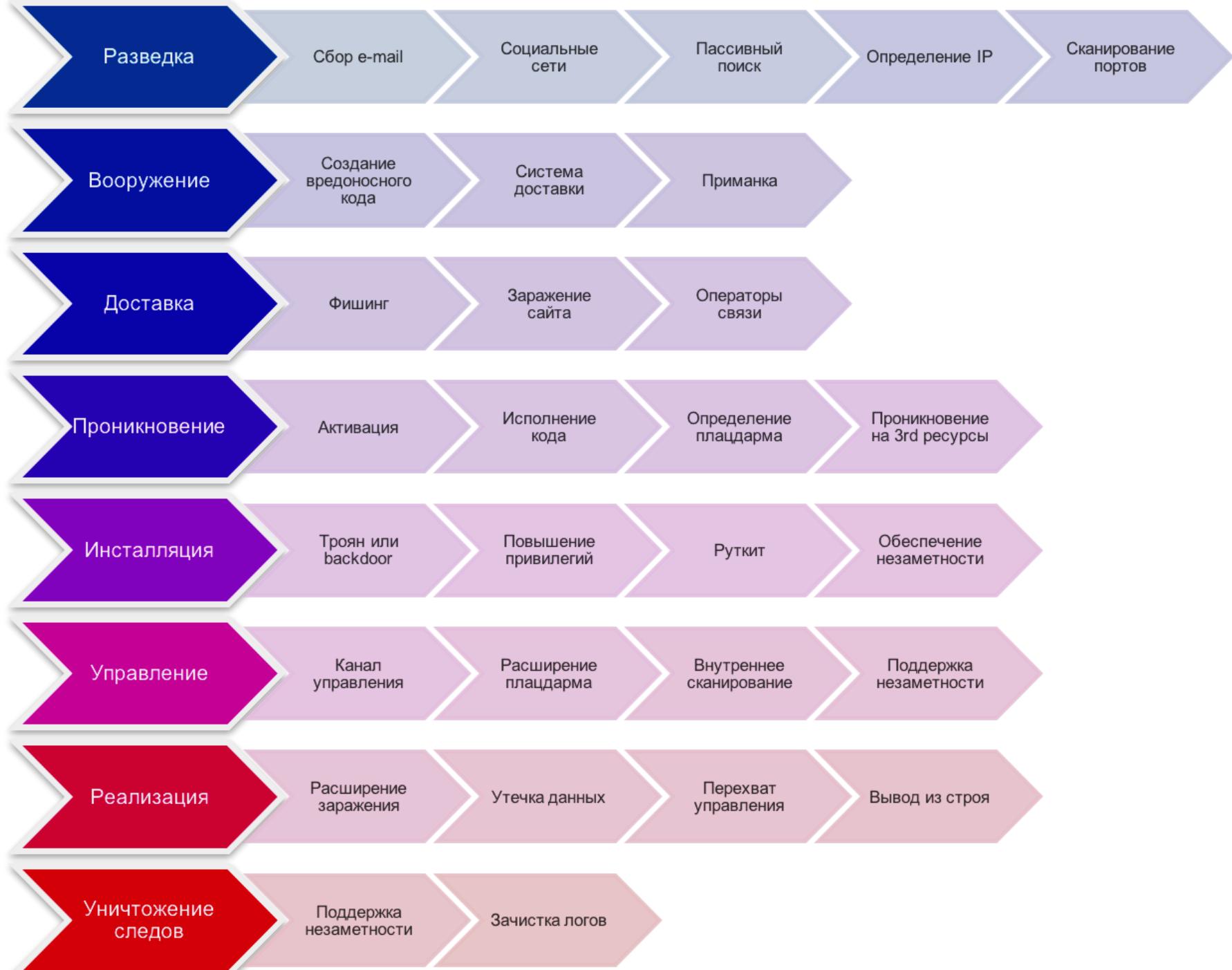
– Реализация
– Получение данных

Реализация последующим управлением

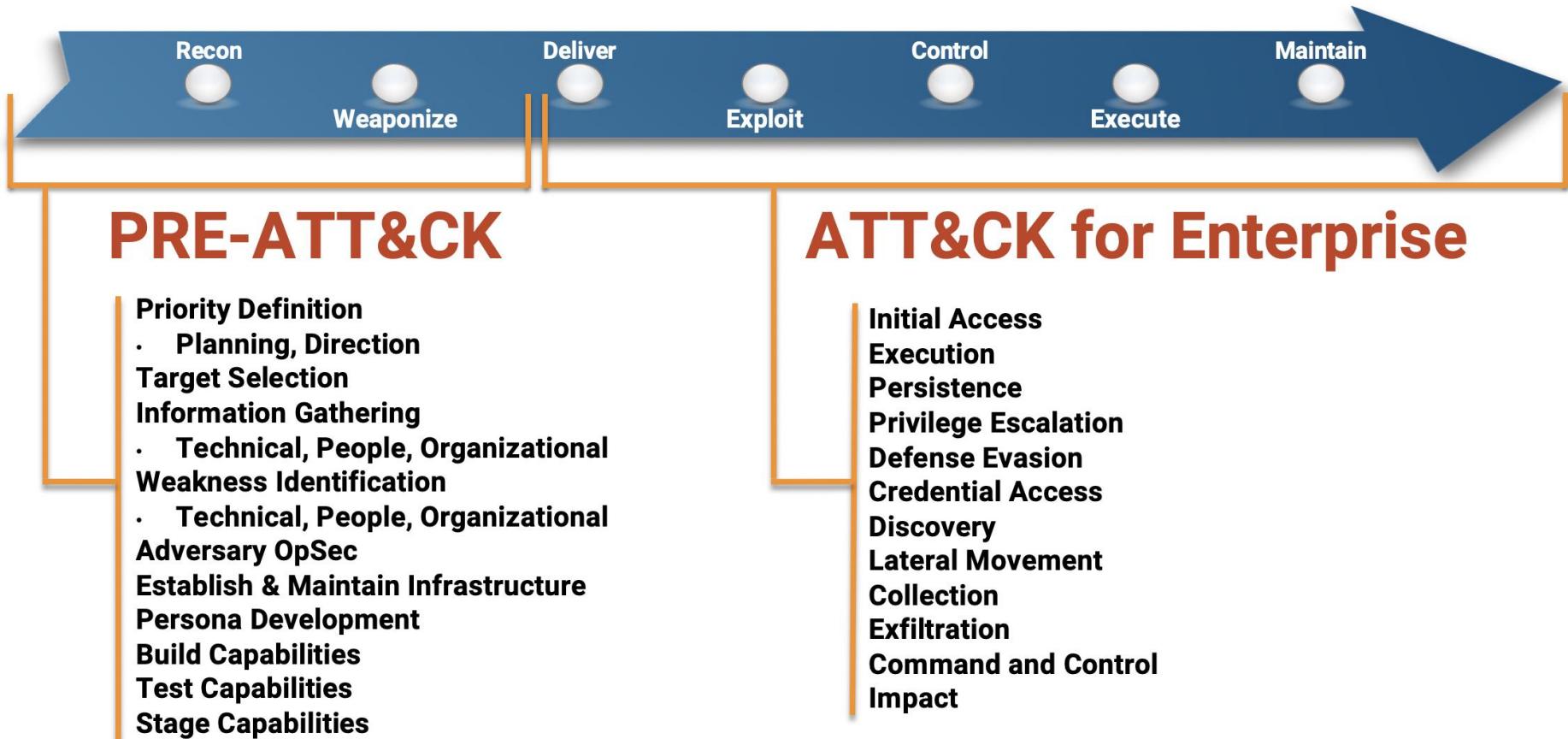
– Фоновый режим

Phases of the Intrusion Kill Chain





Связь с Cyber Kill Chain

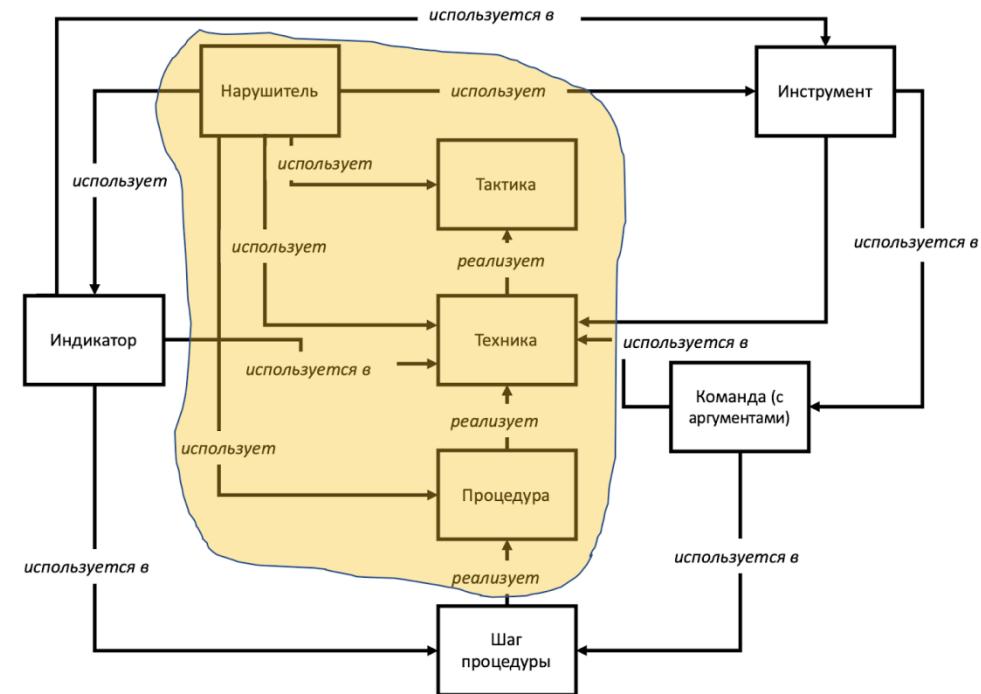


Структура MITRE ATT&CK

Информация в базе знаний MITRE ATT&CK представлена в виде матриц.

Каждая матрица представляет собой таблицу, в которой заголовки столбцов соответствуют *тактикам* киберпреступников, то есть основным этапам кибератаки или подготовки к ней, а содержимое ячеек — *методикам реализации* этих тактик, или *техникам*.

Так, если сбор данных согласно MITRE ATT&CK — это *тактика атаки*, то способы сбора, например автоматический сбор или сбор данных со съемных носителей, — *это техники*.



В базе ATT&CK выделяются 14 тактик, которые разделены по стадиям кибератаки:

- сбор информации (reconnaissance);
- разработка ресурсов (resource development);
- первоначальный доступ (initial access);
- выполнение (execution);
- закрепление (persistence);
- повышение привилегий (privilege escalation);
- предотвращение обнаружения (defense evasion);
- получение учетных данных (credential access);
- разведка (discovery);
- перемещение внутри периметра (lateral movement);
- сбор данных (collection);
- управление и контроль (command and control);
- эксфильтрация данных (exfiltration);
- воздействие (impact).

В базе ATT&CK выделяются 14 тактик, которые разделены по стадиям кибератаки:

attack.mitre.org/tactics/enterprise/

MITRE | ATT&CK®

Tactics

Enterprise

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

Mobile

Home > Tactics > Enterprise

Enterprise

Mobile

Enterprise tactics

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

Enterprise Tactics: 14

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.



Пример Process Injection

MITRE | ATT&CK®

Metrics Tactics Techniques Data Sources Mitigations Groups Software Resources Blog Contribute Search

TECHNIQUES

- Create or Modify System Process
- Domain Policy Modification
- Escape to Host
- Event Triggered Execution
- Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection**
 - Dynamic-link Library Injection
 - Portable Executable Injection
 - Thread Execution Hijacking
 - Asynchronous Procedure Call
 - Thread Local Storage
 - Ptrace System Calls
 - Proc Memory
 - Extra Window Memory Injection
 - Process Hollowing
 - Process Doppelgänging
 - VDSO Hijacking
 - Scheduled Task/Job
 - Valid Accounts
 - Defense Evasion
 - Credential Access
 - Discovery
 - Lateral Movement
 - Collection
 - Command and Control
 - Exfiltration
 - Impact
- Mobile

Home > Techniques > Enterprise > Process Injection

Process Injection

Sub-techniques (11)

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific.

More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

ID: T1055

Sub-techniques: T1055.001, T1055.002, T1055.003, T1055.004, T1055.005, T1055.008, T1055.009, T1055.011, T1055.012, T1055.013, T1055.014

① Tactics: Defense Evasion, Privilege Escalation

② Platforms: Linux, Windows, macOS

③ Defense Bypassed: Anti-virus, Application control

④ CAPEC ID: CAPEC-640

Contributors: Anastasios Pingios; Christiaan Beek, @ChristiaanBeek; Ryan Beccar

Version: 1.2

Created: 31 May 2017

Last Modified: 18 October 2021

[Version Permalink](#)

Procedure Examples

ID	Name	Description
S0469	ABK	ABK has the ability to inject shellcode into svchost.exe. ^[1]
S0331	Agent Tesla	Agent Tesla can inject into known, vulnerable binaries on targeted hosts. ^[2]
G0050	APT32	APT32 malware has injected a Cobalt Strike beacon into Rundll32.exe. ^[3]
G0067	APT37	APT37 injects its malware variant, ROKRAT, into the cmd.exe process. ^[4]
G0096	APT41	APT41 malware TIDYELF loaded the main WINTERLOVE component by injecting it into the iexplore.exe process. ^[5]
S0438	Attor	Attor's dispatcher can inject itself into running processes to gain higher privileges and to evade detection. ^[6]
S0347	AuditCred	AuditCred can inject code from files to other running processes. ^[7]
S0473	Avenger	Avenger has the ability to inject shellcode into svchost.exe. ^[8]
S0093	Backdoor.Oldrea	Backdoor.Oldrea injects itself into explorer.exe. ^[9]

В июле 2020 года добавились подтехники, т. е. более подробные техники. Техники представляют собой широкое действие, предпринимаемое злоумышленником для достижения тактической цели, тогда как подтехника является более конкретным действием противника.

Например, такая техника, как Process Injection, имеет 11 суб-техник, чтобы охватить (более подробно) варианты того, как злоумышленники внедрили код в процессы.

Sub-techniques (11)

ID	Name
T1055.001	Dynamic-link Library Injection
T1055.002	Portable Executable Injection
T1055.003	Thread Execution Hijacking

Матрица ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

Матрица ATT&CK представляет собой полное описание поведения, которое злоумышленники используют при взломе сетей, матрица полезна для различных наступательных и защитных измерений, представлений и других механизмов.

MITRE делит ATT&CK на несколько сводных матриц:

Enterprise — TTP, используемые при атаках на организации;

Mobile — TTP, связанные с переносными устройствами;

ICS — Industrial Control Systems, TTP для индустриальных систем.

В каждой из них — тактики и техники, связанные с предметом этой матрицы.

Самая популярная матрица — Enterprise. Она, в свою очередь, состоит из ответвлений, ответственных каждое за свое:

PRE Matrix — предварительные этапы атаки;

Windows — атаки на инфраструктуры на основе Windows;

macOS — для устройств Apple и MAC;

Linux — для устройств на базе Linux;

Cloud — атаки на облака;

Network — атаки на сеть.

В PRE Matrix содержатся данные, которые касаются подготовительных этапов атаки, например сканирование и инвентаризация сети, фишинг или социальная инженерия. А остальные подтаблицы матрицы Enterprise содержат следующие шаги атаки.

PRE Matrix

Other ATT&CK Enterprise sub-martixes

RECON

WEAPONIZE

DELIVER

EXPLOIT

INSTALL

CONTROL

OBJECTIVE

Матрица ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)-техники

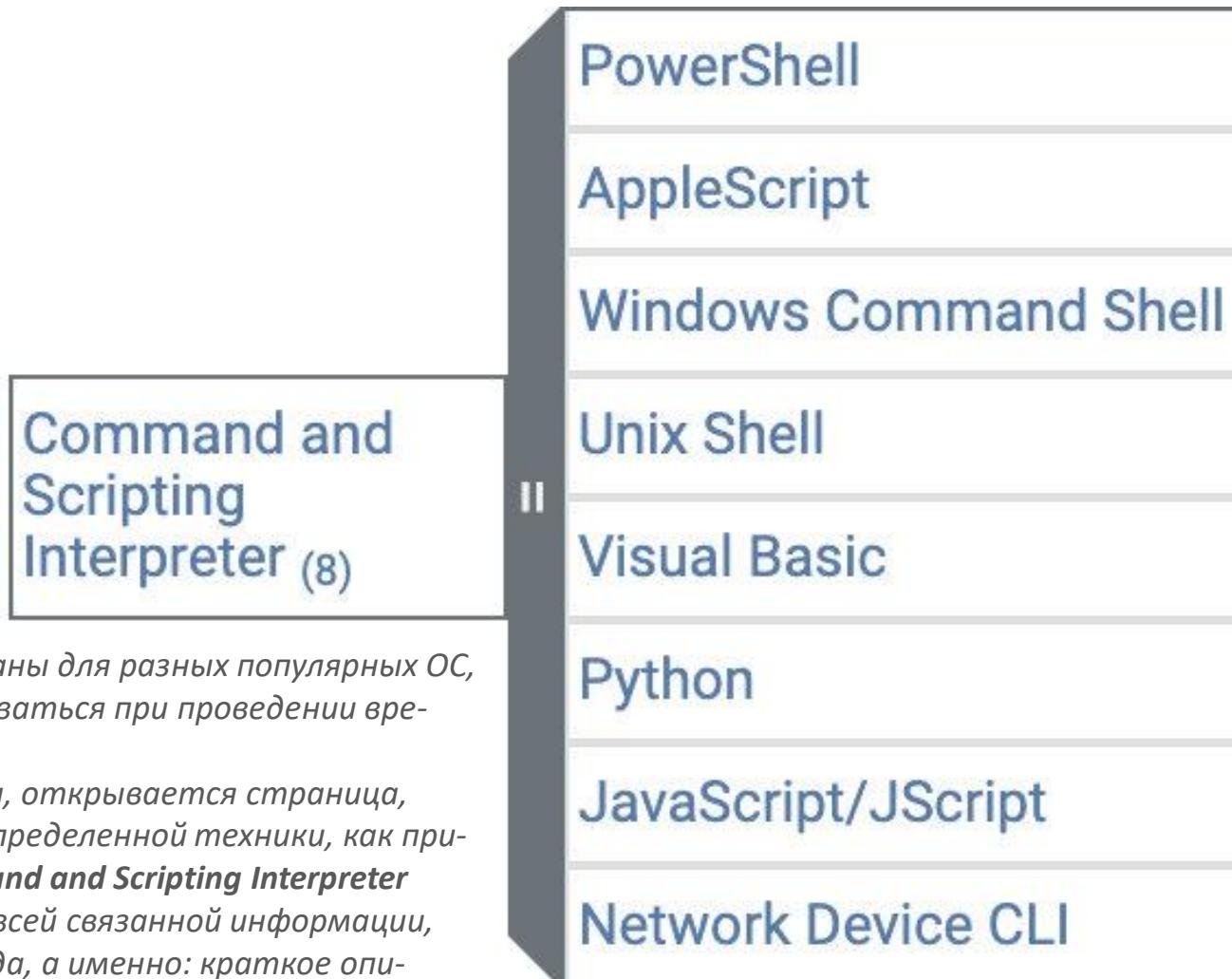
PRE Matrix		Other ATT&CK Enterprise sub-martixes					
RECON	WEAPONIZE	DELIVER	EXPLOIT	INSTALL	CONTROL	OBJECTIVE	
Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	
15 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques	

Категории матрицы ATT&CK Enterprise и количество вложенных техник в каждой категории

Тактика TA0002 Execution содержит следующие техники (у техники могут быть свои подтехники) :

- T1059 — Command and Scripting Interpreter, командные и скриптовые интерпретаторы;
- T1203 — Exploitation for Client Execution, использование уязвимостей в клиентском ПО;
- T1559 — Inter-Process Communication, использование межпроцессного взаимодействия;
- T1106 — Native API, взаимодействие с API операционной системы;
- T1053 — Scheduled Task/Job, жизнь в планировщиках;
- T1129 — Shared Modules, загрузка DLL;
- T1072 — Software Deployment Tools, использование систем развертывания ПО;
- T1569 — System Services, применение служб;
- T1204 — User Execution, действия пользователя, направленные на удобство злоумышленника;
- T1047 — Windows Management Instrumentation, использование WMI.

Матрица ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) - подтехники



Скрипты и команды указаны для разных популярных ОС, которые могут использоваться при проведении вредоносной кампании.

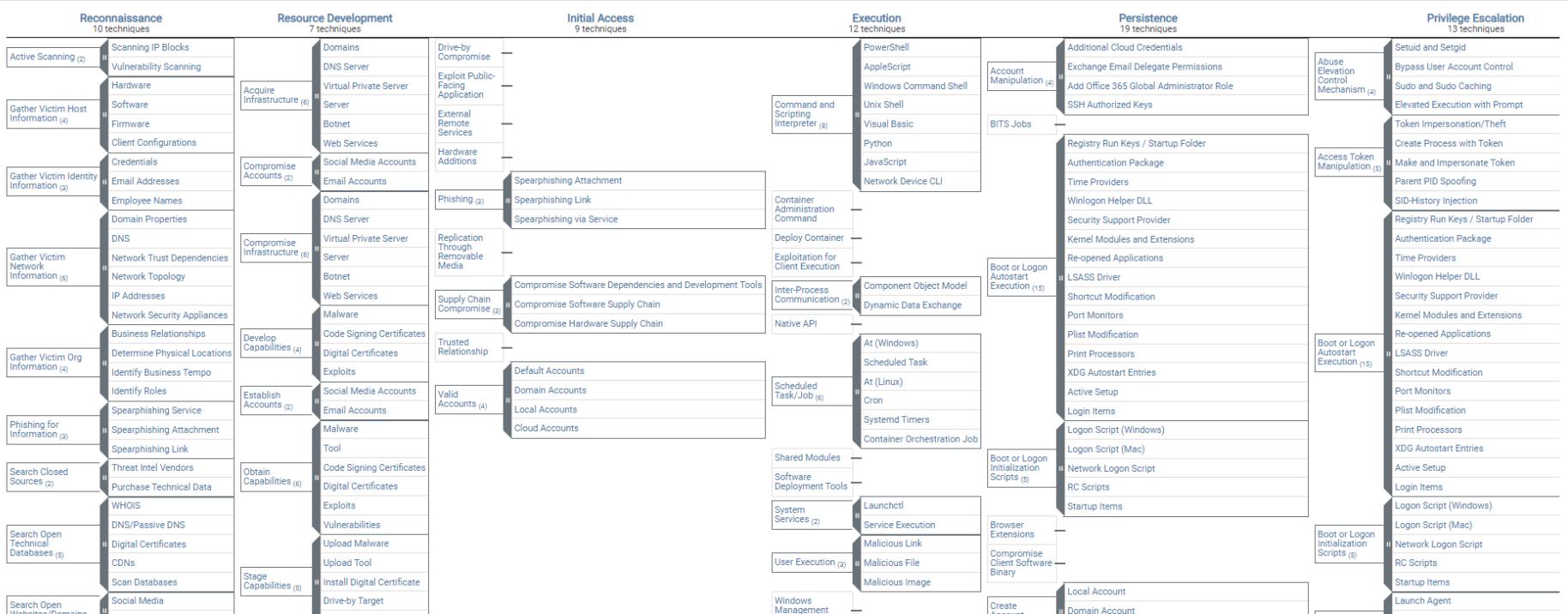
Если кликнуть по надписи, открывается страница, посвященная описанию определенной техники, как пример — по клику на **Command and Scripting Interpreter** открывается доступ ко всей связанной информации, касающейся этого метода, а именно: краткое описание техники, примеры процедур по различным группировкам и меры для снижения рисков.

Подтехники T1059 Command and Scripting Interpreter

Матрица ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – общий вид матрицы

ATT&CK Matrix for Enterprise

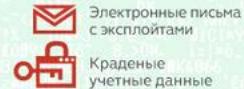
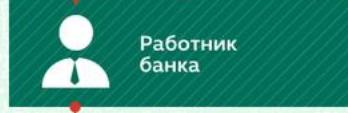
layout: side ▾ show sub-techniques hide sub-techniques



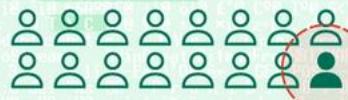
APT-группировка Carbanak

Как кибербанда Carbanak украла миллиард долларов Целевая атака на банк

1. Заражение



Сотни машин заражены в поисках компьютера администратора



2. Сбор разведданных

Перехват данных с экранов служащих



Запись

3. Действия от имени сотрудников

Как были украдены средства

Онлайн-банкинг

Перевод средств на счета мошенников

Системы электронных платежей

Перевод средств в китайские и американские банки

Завышение баланса счетов

Присвоение «лишних» средств через фальшивую транзакцию

Управление банкоматами

Приказы на выдачу наличных в заранее определенное время

На компьютер жертвы устанавливался бэкдор, основанный на коде Carberp, — собственно, отсюда и происходит название данной кампании — Carbanak.

Карта заражений Carbanak

Атаковано более 300 IP-адресов почти в 30 странах мира.



Матрица ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – Carbanak

Чтобы выделить используемые техники, тактики и процедуры, после анализа вредоносной программы можно воспользоваться **MITRE ATT&CK Navigator**. Для примера можно посмотреть разложение целевой атаки Carbanak на ТТР.

*Carbanak - это киберпреступная группа, которая использовала вредоносное ПО Carbanak для нацеливания на финансовые учреждения как минимум с 2013 года. Carbanak может быть связан с группами, отслеживаемыми отдельно как Cobalt Group и FIN7 , которые также использовали вредоносное ПО Carbanak .

Группы: <https://attack.mitre.org/groups/G0008/>

https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0008%2FG0008-enterprise-layer.json

Techniques Used

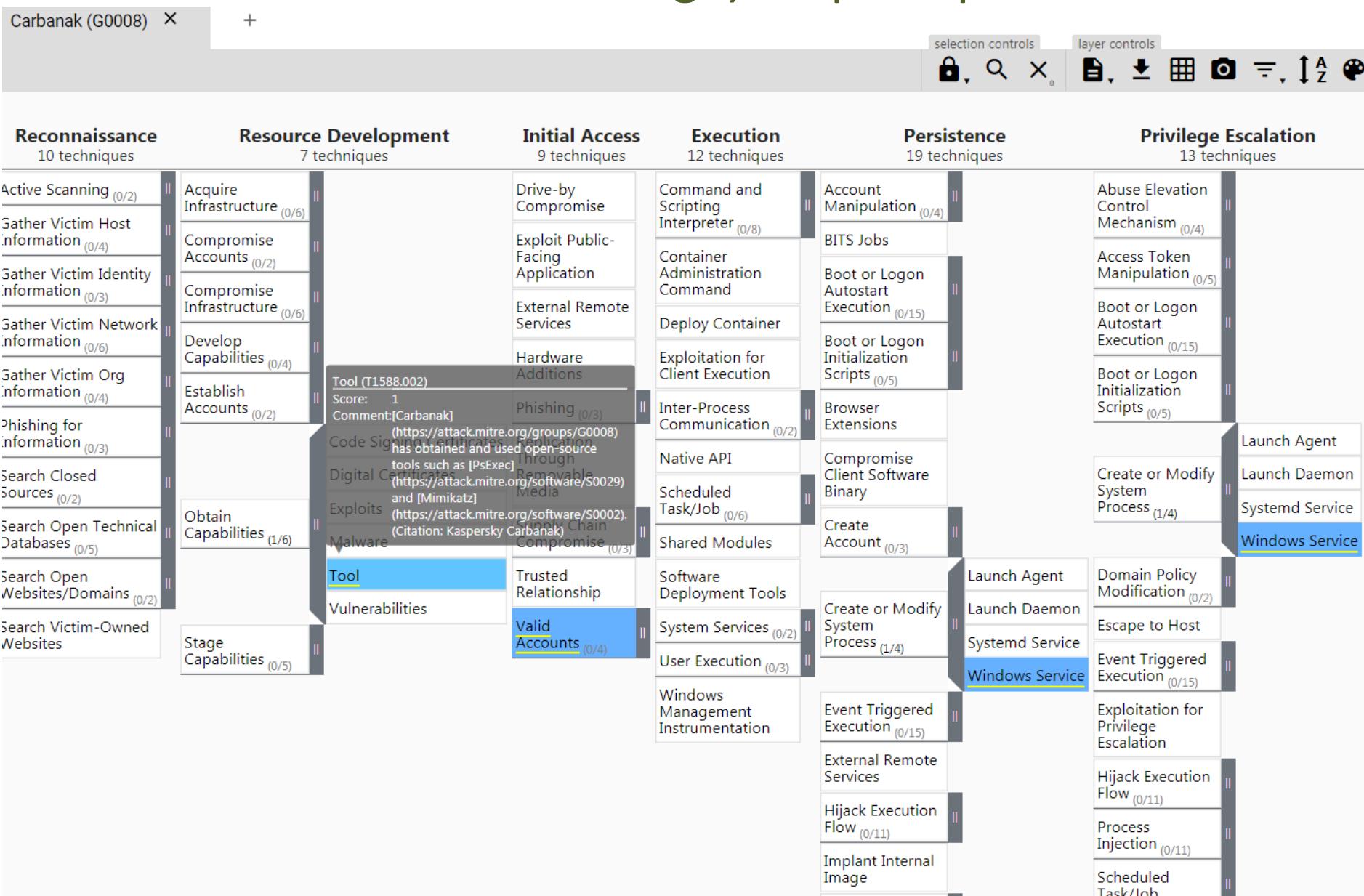
ATT&CK® Navigator Layers ▾

Domain	ID	Name	Use
Enterprise	T1543	.003 Create or Modify System Process: Windows Service	Carbanak malware installs itself as a service to provide persistence and SYSTEM privileges. ^[1]
Enterprise	T1562	.004 Impair Defenses: Disable or Modify System Firewall	Carbanak may use netsh to add local firewall rule exceptions. ^[7]
Enterprise	T1036	Masquerading: Masquerade Task or Service	Carbanak has copied legitimate service names to use for malicious services. ^[1]
		.005 Masquerading: Match Legitimate Name or Location	Carbanak has named malware "svchost.exe," which is the name of the Windows shared service host program. ^[1]
Enterprise	T1588	.002 Obtain Capabilities: Tool	Carbanak has obtained and used open-source tools such as PsExec and Mimikatz. ^[1]
Enterprise	T1219	Remote Access Software	Carbanak used legitimate programs such as AmmyyAdmin and Team Viewer for remote interactive C2 to target systems. ^[7]
Enterprise	T1218	.011 Signed Binary Proxy Execution: Rundll32	Carbanak installs VNC server software that executes through rundll32. ^[1]
Enterprise	T1078	Valid Accounts	Carbanak actors used legitimate credentials of banking employees to perform operations that sent them millions of dollars. ^[1]
Enterprise	T1102	.002 Web Service: Bidirectional Communication	Carbanak has used a VBScript named "ggldr" that uses Google Apps Script, Sheets, and Forms services for C2. ^[8]

Software

ID	Name	References	Techniques
S0030	Carbanak	^[1]	Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Commonly Used Port, Create Account: Local Account, Data Encoding: Standard Encoding, Data Transfer Size Limits, Email Collection: Local Email Collection, Encrypted Channel: Symmetric Cryptography, Indicator Removal on Host: File Deletion, Input Capture: Keylogging, Obfuscated Files or Information, OS Credential Dumping, Process Discovery, Process Injection: Portable Executable Injection, Query Registry, Remote Access Software, Remote Services: Remote Desktop Protocol, Screen Capture
S0002	Mimikatz	^[1]	Access Token Manipulation: SID-History Injection, Account Manipulation, Boot or Logon Autostart Execution: Security Support Provider, Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores, Credentials from Password Stores: Windows Credential Manager, OS Credential Dumping: LSASS Memory, OS Credential Dumping: DCSync, OS Credential Dumping: Security Account Manager, OS Credential Dumping: LSA Secrets, Rogue Domain Controller, Steal or Forge Kerberos Tickets: Silver Ticket, Steal or Forge Kerberos Tickets: Golden Ticket, Unsecured Credentials: Private Keys, Use Alternate Authentication Material: Pass the Hash, Use Alternate Authentication Material: Pass the Ticket
S0108	netsh	^[7]	Event Triggered Execution: Netsh Helper DLL, Impair Defenses: Disable or Modify System Firewall, Proxy, Software Discovery: Security Software Discovery
S0029	PsExec	^[1]	Create Account: Domain Account, Create or Modify System Process: Windows Service, Lateral Tool Transfer, Remote Services: SMB/Windows Admin Shares, System Services: Service Execution

Матрица ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – Пример Carbanak



Матрица ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – шифровальщик ProLock Ransomware

— первоначальный доступ (initial access);

Операторы ProLock используют два основных вектора первичной компрометации: вредоносное ПО, троян QakBot (Qbot) и незащищенные RDP-серверы со слабыми паролями. QakBot распространяется через фишинговые кампании. Фишинговое письмо может содержать прикрепленный документ Microsoft Office или ссылку на такой файл, находящийся в облачном хранилище, например, Microsoft OneDrive.

— выполнение (execution);

После загрузки и открытия зараженного документа пользователю предлагается разрешить выполнение макросов, в случае успеха осуществляется запуск PowerShell, который позволит загрузить и запустить полезную нагрузку QakBot с командного сервера.

Важно отметить, что тоже самое относится и к ProLock: полезная нагрузка извлекается из файла BMP или JPG и загружается в память с помощью PowerShell. В некоторых случаях для запуска PowerShell используется запланированная задача (Batch-скрипт, запускающий ProLock через планировщик задач):

```
schtasks.exe /CREATE /XML C:\Programdata\WinMgr.xml /tn WinMgr  
schtasks.exe /RUN /tn WinMgr  
del C:\Programdata\WinMgr.xml  
del C:\Programdata\run.bat
```

— закрепление в системе (persistence);

В случае получения доступа путем компрометации RDP-сервера для закрепления в сети используются действующие учетные записи. Для QakBot характерны разнообразные механизмы закрепления. Чаще всего данный троян использует раздел реестра Run и создает задачи в планировщике:

Value name	hdeqcrc
Value type	RegSz
Value	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "\$windowsupdate = \"C:\Users\IEUser\AppData\Roaming\Microsoft\Cpdfxoatpg\egvmxii.exe\"; & \$windowsupdate"

Закрепление Qakbot в системе с помощью раздела реестра Run.

В некоторых случаях также используются папки автозагрузки: туда помещается ярлык, который указывает на загрузчик.

— обход защиты, предотвращение обнаружения (defense evasion);

Путем коммуникации с командным сервером QakBot периодически пытается обновить себя, поэтому, чтобы избежать обнаружения, вредонос может заменить собственную текущую версию новой. Исполняемые файлы подписываются скомпрометированной или поддельной подписью. Начальная полезная нагрузка, загружаемая PowerShell, хранится на командном сервере с расширением PNG. Кроме того, после выполнения она заменяется на легитимный файл calc.exe.

Также, чтобы скрыть вредоносную активность, QakBot использует технику внедрения кода в процессы, используя для этого explorer.exe.

Как уже упоминалось, полезная нагрузка ProLock скрыта внутри файла BMP или JPG. Это также можно рассматривать как метод обхода защиты.

Матрица ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – шифровальщик ProLock Ransomware

— получение учетных данных (credential access);

QakBot обладает функционалом кейлогера. Помимо этого, он может загружать и запускать дополнительные скрипты, например, Invoke-Mimikatz – PowerShell-версию знаменитой утилиты Mimikatz. Такие скрипты могут использоваться злоумышленниками для дампинга учетных данных.

— сетевая разведка (discovery);

После получения доступа к привилегированным учетным записям операторы ProLock осуществляют сетевую разведку, которая в частности может включать в себя сканирование портов и анализ среды Active Directory. Помимо различных скриптов, для сбора информации об Active Directory злоумышленники используют AdFind – еще один инструмент, популярный среди групп, использующих программы-вымогатели.

— перемещение внутри периметра, продвижение по сети (lateral movement);

Традиционно одним из самых популярных способов продвижения по сети является протокол удаленного рабочего стола (Remote Desktop Protocol). ProLock не стал исключением. Злоумышленники имеют скрипты для получения возможности удаленного доступа по протоколу RDP к целевым хостам:

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0 /f  
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes  
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "UserAuthentication" /t  
REG_DWORD /d 0 /f
```

Использование BAT скрипта для получения доступа по протоколу RDP

Для удаленного выполнения скриптов операторы ProLock используют еще один популярный инструмент – утилиту PsExec из пакета Sysinternals Suite.

Запуск ProLock на хостах осуществляется с помощью WMIC, представляющего собой интерфейс командной строки для работы с подсистемой Windows Management Instrumentation. Данный инструмент также приобретает все большую популярность среди операторов программ-вымогателей.

Матрица ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – шифровальщик ProLock Ransomware

— **сбор данных (collection);**

Как и многие другие операторы шифровальщиков, группа, использующая ProLock, собирает данные из скомпрометированной сети, чтобы повысить свои шансы на получение выкупа. Перед эксфильтрацией собранные данные архивируются с помощью утилиты 7Zip.

— **эксфильтрация (exfiltration);**

Для выгрузки данных операторы ProLock используют Rclone – инструмент командной строки, предназначенный для синхронизации файлов с различными облачными хранилищами, такими как OneDrive, Google Drive, Mega и др. Злоумышленники всегда переименовывают исполняемый файл, чтобы он был похож на легитимные системные файлы.

В отличие от других злоумышленников, операторы ProLock до сих пор не имеют собственного веб-сайта для публикации украшенных данных, принадлежащих компаниям, которые отказались платить выкуп.

— **достижение конечной цели, управление и контроль (command and control);**

- После эксфильтрации данных группа развертывает ProLock по всей сети предприятия. Бинарный файл извлекается из файла с расширением PNG или JPG с помощью PowerShell и внедряется в память.
- Прежде всего, ProLock завершает процессы, указанные во встроенном списке (интересно, что он использует только шесть букв из имени процесса, например, «winwor»), и завершает службы, включая те, которые связаны с безопасностью, например, CSFalconService (CrowdStrike Falcon), с помощью команды net stop.
- Затем, как и в случае многих других семейств вымогателей, атакующие используют vssadmin для удаления теневых копий Windows и ограничения их размера, благодаря чему новые копии не будут создаваться.
- ProLock добавляет расширение .proLock, .pr0Lock или .proL0ck к каждому зашифрованному файлу и помещает файл [HOW TO RECOVER FILES].TXT в каждую папку. Этот файл содержит инструкции о том, как расшифровать файлы, включая ссылку на сайт, где жертва должна ввести уникальный идентификатор и получить платежную информацию.

Hello, you are a victim of ProLock ransomware.

Your files have been encrypted using RSA2048 algorithm.

This algorithm is one of the strongest, it is impossible to decrypt files without known key.

As you understand, situation is very important.

You can decrypt 1-2 files for free as a proof of work.

We know that this computer is very valuable for you.

So we will give you appropriate price for recovering.

DON'T try to change files by yourself, DON'T use any third party software for restoring your data or antivirus solutions - these actions may entail damage of the private key and, as result, the loss of all your data.

All your sensitive data was downloaded on remote servers. If you do not pay in several days all these sensitive files will be published in social networks and public media.

To get your files unlocked, pay.

If you want to make test unlock, contact support.

Payment information

35 BTC

UNPAID

Каждый экземпляр ProLock содержит информацию о сумме выкупа – в данном случае это 35 биткоинов, что составляет примерно 312 000 долларов США.

MITRE ATT&CK Mapping

Для автоматизации маппинга можно использовать официальный инструмент Threat Report ATT&CK Mapper (TRAM), который с помощью механизмов NLP (обработка текстов на естественном языке) по ключевым словам предлагает соответствующую тактику или технику.

Tactic	Technique
Initial Access (TA0001)	External Remote Services (T1133), Spearphishing Attachment (T1193), Spearphishing Link (T1192)
Execution (TA0002)	Powershell (T1086), Scripting (T1064), User Execution (T1204), Windows Management Instrumentation (T1047)
Persistence (TA0003)	Registry Run Keys / Startup Folder (T1060), Scheduled Task (T1053), Valid Accounts (T1078)
Defense Evasion (TA0005)	Code Signing (T1116), Deobfuscate/Decode Files or Information (T1140), Disabling Security Tools (T1089), File Deletion (T1107), Masquerading (T1036), Process Injection (T1055)
Credential Access (TA0006)	Credential Dumping (T1003), Brute Force (T1110), Input Capture (T1056)
Discovery (TA0007)	Account Discovery (T1087), Domain Trust Discovery (T1482), File and Directory Discovery (T1083), Network Service Scanning (T1046), Network Share Discovery (T1135), Remote System Discovery (T1018)
Lateral Movement (TA0008)	Remote Desktop Protocol (T1076), Remote File Copy (T1105), Windows Admin Shares (T1077)
Collection (TA0009)	Data from Local System (T1005), Data from Network Shared Drive (T1039), Data Staged (T1074)
Command and Control (TA0011)	Commonly Used Port (T1043), Web Service (T1102)
Exfiltration (TA0010)	Data Compressed (T1002), Transfer Data to Cloud Account (T1537)
Impact (TA0040)	Data Encrypted for Impact (T1486), Inhibit System Recovery (T1490)

ПРАВИЛА CAPA

Разрешения, которые запрашивает при установке почти любое приложение для *Android*, давно привлекают внимание ИБ-специалистов. Обычно просят и доступ к камере, и к микрофону, и к сети. Исследователям из *FireEye* это понравилось — какие возможности есть у определенного исполняемого файла?

<https://github.com/mandiant/capa-rules>

При динамическом анализе объекта он запускается в изолированной среде и мониторится вся активность на уровне гипервизора или специальных утилит. Используя CAPA-правила (open-source), аналитик может сократить время, провести предварительный статический анализ объекта и сконцентрироваться на потенциальных активностях и возможностях программы по матрице MITRE ATT&CK.

Вывод CAPA при анализе .exe. Программа была написана на Python и собрана в исполняемый файл с помощью *auto_py_to_exe*.

```
C:\Users\poc\Desktop\capa-master>capa.exe -r rules\capa-rules-master "C:\Users\poc\1.exe"
loading : 100%|#####| 343/343 [00:03<00:00, 103.03      rules/s]
matching: 100%|#####| 1289/1289 [00:29<00:00, 43.79 functions/s]
+-----+
| md5          | b261c95de9f719d6334fdb49644fb545
| sha1         | 5bcc53495884f135b86fb15b52802196d9eb6c2
| sha256       | f56c81607f0cc15622b36f015c0663f2db396b1da08a79fb3209a9431db214e2
| path         | C:\Users\poc\1.exe
+-----+
+-----+
| ATT&CK Tactic | ATT&CK Technique
|-----+
| DEFENSE EVASION | Obfuscated Files or Information [T1027]
|                   | Virtualization/Sandbox Evasion::System Checks [T1497.001]
| DISCOVERY        | File and Directory Discovery [T1083]
|                   | System Information Discovery [T1082]
| EXECUTION        | Shared Modules [T1129]
+-----+
```

Анализируемый файл использует три тактики и пять техник по матрице MITRE ATT&CK.

Помимо этого, CAPA выводит список возможностей исполняемого файла по используемым функциям.

ПРАВИЛА САРА

CAPABILITY	NAMESPACE
check for time delay via GetTickCount	anti-analysis/anti-debugging/debugger-detection
execute anti-VM instructions (4 matches)	anti-analysis/anti-vm/vm-detection
reference anti-VM strings targeting Xen	anti-analysis/anti-vm/vm-detection
hash data with CRC32	data-manipulation/checksum/crc32
encode data using XOR (26 matches)	data-manipulation/encoding/xor
decrypt data using AES via x86 extensions	data-manipulation/encryption/aes
hash data using murmur3	data-manipulation/hashing/murmur
hash data using SHA1	data-manipulation/hashing/sha1
hash data using SHA256 (2 matches)	data-manipulation/hashing/sha256
contains PDB path	executable/pe/pdb
contain a resource (.rsrc) section	executable/pe/section/rsrc
accept command line arguments (3 matches)	host-interaction/cli
interact with driver via control codes	host-interaction/driver
query environment variable (2 matches)	host-interaction/environment-variable
set environment variable (2 matches)	host-interaction/environment-variable
get common file path (4 matches)	host-interaction/file-system
create directory (2 matches)	host-interaction/file-system/create
delete directory	host-interaction/file-system/delete
delete file (3 matches)	host-interaction/file-system/delete
check if file exists (5 matches)	host-interaction/file-system/exists
enumerate files via kernel32 functions (2 matches)	host-interaction/file-system/files/list
get file attributes (3 matches)	host-interaction/file-system/meta
set file attributes (2 matches)	host-interaction/file-system/meta
move file (2 matches)	host-interaction/file-system/move
read file (2 matches)	host-interaction/file-system/read
read file via mapping	host-interaction/file-system/read
bypass Windows File Protection	host-interaction/file-system/windows-file-protection
write file (6 matches)	host-interaction/file-system/write
get system information	host-interaction/os/info
allocate thread local storage	host-interaction/process
get thread local storage value (2 matches)	host-interaction/process
set thread local storage value (2 matches)	host-interaction/process
terminate process (4 matches)	host-interaction/process/terminate
create thread	host-interaction/thread/create
link function at runtime (3 matches)	linking/runtime-linking
parse PE header (8 matches)	load-code/pe

САРА выводит список возможностей исполняемого файла по используемым функциям.

ПРАВИЛА CAPA

Автоматическое определение возможностей в CAPA реализовано через поиск характерных артефактов. Это используемые вызовы API, строки, константы, создание мьютексов и сокетов, подгружаемые либы. Эти артефакты задаются правилами (похожими на правила YARA), которые помогают выявить функции, реализованные во вредоносе.

Рассмотрим пример правила CAPA.

```
rule:
  meta:
    name: schedule task via command line
    namespace: persistence/scheduled-tasks
    author: 0x534a@mailbox.org
    scope: function
    att&ck:
      - Persistence::Scheduled Task/Job::Scheduled Task [T1053.005]
    examples:
      - 79cded1aa711e321b4939805d27e160be:0x401440
  features:
    - and:
      - match: create process
      - or:
        - and:
          - string: /schtasks/i
          - string: /\create /i
        - string: /Register-ScheduledTask /i
```

В первую очередь CAPA извлекает строки и константы, которые могут быть именами функций или о чем-то говорить эксперту. Найденное разделяется на файловые свойства и результаты дизассемблирования (строки, константы, вызовы). Файловые свойства — это заголовки и импортируемые API (в том числе названий используемых функций).

создание_процесса И [(строка /schtasks/i И строка /\create /i) ИЛИ строка /Register-ScheduledTask /i]

То есть правило детектирует консольные команды, с помощью которых создаются задачи в планировщике Windows.

Выводы MITRE ATT&CK

Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control
Process Injection	Process Hollowing	Steal Web Session Cookie	Software Discovery	Email Collection	Standard Application Layer Protocol
	Process Injection	Credentials from Web Browsers	Virtualization/Sandbox Evasion		
	DLL Side-Loading	Credentials in Registry	Query Registry		
	Virtualization/Sandbox Evasion	Credentials in Files	Browser Bookmark Discovery		
	File Deletion				

- Матрица позволяет строить модели угроз для разных типов компаний и показывать, какие из известных угроз можно закрыть конкретными решениями.
- Профиль кибергруппировок и их кампаний по MITRE ATT&CK помогает понять, какие инструменты используют злоумышленники, ознакомиться с их техниками и тактиками. Эти знания позволяют прогнозировать вероятную точку входа в организации.
- Активное и повсеместное применение базы знаний ATT&CK позволит унифицировать подход всего сообщества кибербезопасности — как бы поможет говорить на общем языке.
- Матрица строится на основе уже проведенных атак и дает поведенческую справку о том, какие TTP использовались.