**Санкт-Петербургский политехнический университет Петра Великого**
Институт компьютерных наук и технологий
Кафедра компьютерных систем и программных технологий

# РЕФЕРАТ

Основные новые угрозы информационной безопасности 2017 года

(тема работы)

Защита информации

(наименование дисциплины)

**Работу выполнили:**

Волкова М.Д.

подпись Ф.И.О.

**Преподаватель:**

Новопашенный А.Г.

подпись Ф.И.О.

Санкт-Петербург
2018

# Введение

XXI век характеризуется все более широким использованием информационных технологий в жизни общества. Широкое проникновение социальных сетей, использование Интернет как основного источника информации внесли серьезные изменения в социальные отношения в мире.

Сегодня информационные технологии дают возможность людям из различных стран и континентов обсуждать интересующие их проблемы в режиме реального времени. Современные информационные технологии позволяют получать информацию непосредственно с места событий или от лиц, принимавших участие.

Все крупные мировые СМИ сегодня уже имеют представительство в Интернет, и у нас есть уникальная возможность получать информацию из различных источников, формируя полное представление о происходящем, понимая через это общение различие в культурах.

В целом, формируется новая среда - информационная, в которой очень сложно разрешаются различные взаимодействия. Данная среда является многоуровневой, и каждый из уровней в свою очередь также представляет собой ряд нетривиальных технических решений. Естественно, из-за сложности организации, а также ценности информации, вокруг которой построена данная среда, возникают различные методы воздействия на среду и информацию, которые влекут за собой выгодные кому-то последствия. Методы воздействия на среду или на информацию в данной среде очень часто являются не легитимными и носят исключительно корыстный характер и имеют серьезные последствия. Поэтому очень важно иметь представление о возможных опасностях, грозящих нашей информации или всей среде в целом. Возможные опасности – это не что иное как угрозы. Именно об угрозах в области информационной безопасности и пойдет речь далее.

## Классификация угроз

Основными видами угроз безопасности информационных технологий и информации (угроз интересам субъектов информационных отношений) являются:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т. п.);
- сбои и отказы оборудования (технических средств) АИТУ;
- последствия ошибок проектирования и разработки компонентов АИТУ (аппаратных средств, технологии обработки информации, программ, структур данных и т. п.);
- ошибки эксплуатации (пользователей, операторов и другого персонала);
- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т. п.).

Угрозы безопасности можно классифицировать по различным признакам.
По результатам акции:

- угроза утечки;
- угроза модификации;
- угроза утраты.

По нарушению свойств информации:

- угроза нарушения конфиденциальности обрабатываемой информации;
- угроза нарушения целостности обрабатываемой информации;
- угроза нарушения работоспособности системы (отказ в обслуживании), т. е. угроза доступности.

По природе возникновения:

- естественные;
- искусственные.

**Естественные угрозы** — это угрозы, вызванные воздействиями на компьютерную систему и ее элементы объективных физических процессов или стихийных природных явлений.
**Искусственные угрозы** — это угрозы компьютерной системе, вызванные деятельностью человека. Среди них, исходя и мотивации действий, можно выделить:

- **непреднамеренные** (неумышленные, случайные) угрозы, вызванные ошибками в проектировании компьютерной системы и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т. п.;
- **преднамеренные** (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников). Источники угроз по отношению к информационной технологии могут быть внешними или внутренними (компоненты самой компьютерной системы - ее аппаратура, программы, персонал).

Основные непреднамеренные искусственные угрозы (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т. п.);
- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- неумышленная, порча носителей информации;
- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т. п.);
- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- заражение компьютера вирусами;
- неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. п.).
- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими угрозу для работоспособности системы и безопасности информации;
- игнорирование организационных ограничений (установленных правил) при ранге в системе;
- вход в систему в обход средств зашиты (загрузка посторонней операционной системы со сменных магнитных носителей и т. п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

Основные преднамеренные искусственные угрозы характеризуются возможными путями умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

- физическое разрушение системы (путем взрыва, поджога и т. п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т. п.);
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т. п.);
- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т. п.);
- внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
- вербовка (путем подкупа, шантажа и т. п.) персонала или отдельных пользователей, имеющих определенные полномочия;
- применение подслушивающих устройств, дистанционная фото- и видеосъемка и т. п.;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводка активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т. п.);
- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
- хищение носителей информации (дисков, флешеклент, микросхем памяти, запоминающих устройств и персональных ЭВМ);
- несанкционированное копирование носителей информации;
- хищение производственных отходов (распечаток, записей, списанных носителей информации и т. п.);
- чтение остатков информации из оперативной памяти и с внешних запоминающих устройств;
- чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных операционных систем и систем программирования;
- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, имитации интерфейса системы и т. п.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие, как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т. п.;

- вскрытие шифров криптозащиты информации;
- внедрение аппаратных спецвложений, программ «закладок» и «вирусов» («троянских коней» и «жучков»), т. е. таких участков программ, которые не нужны для осуществления заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
- незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один способ, а их некоторую совокупность из перечисленных выше.

## Обзор

Cisco 2018 Annual Cybersecurity Report

Вредоносное ПО не перестает совершенствоваться: сегодня злоумышленники используют облачные сервисы и избегают обнаружения с помощью шифрования, которое помогает скрыть активность потока команд и управления. По данным 11-го отчета Cisco по кибербезопасности (Cisco 2018 Annual Cybersecurity Report, [1]), чтобы сократить время обнаружения злоумышленников, специалисты по кибербезопасности начинают все больше применять (и закупать) средства, использующие искусственный интеллект (ИИ) и машинное самообучение (МС).

С одной стороны, шифрование помогает усилить защиту, с другой — рост объемов как легитимного, так и вредоносного шифрованного трафика (50% по состоянию на октябрь 2017 г.) множит проблемы для защищающихся в процессе выявления потенциальных угроз и мониторинга их активности. За прошедшие 12 месяцев специалисты Cisco по информационной безопасности зафиксировали более чем трехкратный рост шифрованного сетевого трафика от инспектируемых образцов вредоносного ПО.

Применение машинного самообучения помогает повысить эффективность защиты сети и с течением времени позволит автоматически выявлять нестандартные паттерны в шифрованном веб-трафике, в облачных и IoT-средах. Некоторые из 3600 директоров по информационной безопасности, опрошенных в ходе подготовки отчета Cisco 2018 Security Capabilities Benchmark Study, заявили, что доверяют таким инструментам, как МС и ИИ, и хотели бы их использовать, но они разочарованы большим количеством ложных срабатываний. Технологии МС и ИИ, которые сейчас находятся в самом начале своего развития, с течением времени усовершенствуются и научатся определять «нормальную» активность сетей, мониторинг которых они осуществляют.

Финансовый ущерб от атак все более реален. По данным респондентов, более половины всех атак нанесли финансовый ущерб в размере свыше 500 млн долларов, включая в том числе потерю доходов, отток заказчиков, упущенную выгоду и прямые издержки.
Атаки на цепочки поставок усложняются и набирают скорость

- Такие атаки способны масштабно поражать компьютеры, при этом их действие может продолжаться месяцы и даже годы. Необходимо помнить о потенциальных рисках использования программного и аппаратного обеспечения организаций, которые не воспринимают серьезно вопросы информационной безопасности.
- В 2017 г. две подобные атаки заражали пользователей вирусами Nyetya и Ccleaner через доверенное ПО.

- Для снижения рисков атаки на цепочку поставок необходимо пересматривать процедуры сторонних организаций для тестирования эффективности технологий информационной безопасности.

Защищать становится все сложнее, уязвимости становятся разнообразнее Для своей защиты организации используют комплексные сочетания продуктов от различных производителей. Такое усложнение при расширяющемся разнообразии уязвимостей отрицательно сказывается на способность организаций к отражению атаки и ведет в том числе к увеличению рисков финансовых потерь.

- В 2017 г. 25% специалистов по информационной безопасности сообщили, что используют продукты от 11—20 вендоров, в 2016 г. так ответили 18%.
- Специалисты по информационной безопасности сообщили, что 32% уязвимостей затронули более половины систем, в 2016 г. так ответили 15%.

Специалисты по информационной безопасности оценили пользу средств поведенческого анализа для выявления вредоносных объектов

- 92% специалистов считают, что средства поведенческого анализа хорошо справляются с поставленной задачей.
- 2/3 представителей сектора здравоохранения и представители индустрии финансовых услуг считают поведенческую аналитику полезной для выявления вредоносных объектов.

Растет использование облачных технологий; атакующие пользуются отсутствием продвинутых средств обеспечения безопасности

- В этом году 27% специалистов по информационной безопасности сообщили об использовании внешних частных облаков (показатель 2016 г. — 20%).
- Из них 57% размещают сеть в облаке ради лучшей защиты данных, 48% — ради масштабируемости, 46% — ради удобства эксплуатации.
- Хотя облако и обеспечивает повышенную безопасность данных, атакующие пользуются тем, что организации не очень хорошо справляются с защитой развивающихся и расширяющихся облачных конфигураций. Эффективность защиты таких конфигураций повышается с использованием сочетания передовых методик, таких продвинутых технологий безопасности, как машинное самообучение, и таких средств защиты первой линии, как облачные платформы информационной безопасности.

Тенденции роста объемов вредоносного ПО и время обнаружения

- Продемонстрированное Cisco медианное время обнаружения (time to detection, TTD) за период с ноября 2016 по октябрь 2017 г. составило около 4,6 часов. В ноябре 2015 г. этот показатель составил 39 часов, а по данным Отчета Cisco по кибербезопасности за 2017 г., медианное время обнаружения за период с ноября 2015 по октябрь 2016 г. составило 14 часов.
- Ключевым фактором для Cisco в процессе сокращения времени обнаружения и поддержания его на низком уровне стали облачные технологии обеспечения информационной безопасности. Чем меньше время обнаружения, тем быстрее отражается атака.

## Security Intelligence Report 2017: Microsoft

По данным Microsoft[2], в 1 квартале 2017 года примерно на 15% компьютеров в России было зафиксировано вредоносное ПО, в мире этот показатель составил 9%. Годом ранее было отмечено почти в два раза больше подобных инцидентов: 27,2% — в России, 18,3% — в мире. Количество атак на облачные сервисы по всему миру увеличилось на 300%.

Согласно исследованию, по итогам 1 квартала 2017 года 14,8% компьютеров в России столкнулись с вредоносным ПО, тогда как в мире этот показатель составил 9%. При этом статистика по месяцам в России за отчетный квартал демонстрирует тенденцию к снижению — 17,2% в январе, 15,1% в феврале и 12% в марте 2017 года*.
Данные угрозы были зафиксированы и предотвращены системой безопасности Windows Defender Security Intelligence (WDSI), которая ежемесячно сканирует по всему миру более 400 миллиардов электронных писем на наличие фишинговых атак и вредоносного ПО, анализирует 450 миллиардов попыток входа в учетную запись и проверяет более 18 миллиардов веб-страниц.

С ростом популярности облачных сервисов увеличилось и количество атак на них. По данным исследования Microsoft, за 1 квартал 2017 года в мире было зафиксировано в 4 раза больше угроз безопасности, чем за аналогичный период годом ранее. Количество попыток входа в учетную запись Microsoft с вредоносных IP-адресов увеличилось на 44%, став самой главной причиной заражения облачных сервисов (51%). Также наиболее распространены атаки через: протокол удалённого доступа (23%), спам (19%), сканирование портов (3,7%), протокол SSH* (1,7%) и другие. Более 2/3 атак на сервисы Microsoft Azure за первый квартал 2017 года было совершенно с IP-адресов в Китае (35,1%) и США (32,5%). На 3-м месте — Южная Корея (3,1%).

Инструменты защиты Microsoft каждый день автоматически обнаруживают миллионы попыток взлома паролей и блокируют их. Azure Security Center дает полный контроль над безопасностью облачных сервисов Azure. Используя инновационные технологии машинного обучения и больших данных, он своевременно обнаруживает и реагирует на угрозы, а также дает рекомендации по повышению уровня
В отчете отмечается, что самой распространенной категорией стали трояны: на конец 1 квартала 2017 года они были обнаружены у пользователей 10,26% компьютеров. Второе и третье место заняли вирусы (1,59%) и загрузчики троянов и дропперы (0,64%). В тот же период среди нежелательного программного обеспечения на большинстве зараженных компьютеров были найдены инсталляторы дополнительного ПО (5,49%), модификаторы браузера (2,14%) и рекламное ПО (0,25%).

## Основные события

### Шифровальщики

Вирусы-шифровальщики уже сами по себе давно не новость, однако на их долю в текущем году выпало очень много инцидентов и шумихи вокруг этого. И не зря.. случившиеся заметным образом отличается от того что было в предыдущие годы.

По статистике некоторых исследований, каждая 10-я компания в 2017 года так или иначе стала жертвой вируса-шифровальщика. При этом, средний срок обнаружения взлома системы составляет 172 дня на Западе и почти 3 года в России. Если подойти с юмором, то вполне можно сказать, что 2017 это год шифровальщиков - майский WannaCry, летний ExPetr и осенний BadRabbit. Так по масштабам WannaCry и вовсе можно сравнить разве что с всемирным распространением червя Conficker в 2008-2009 году, что в антивирусных энциклопедиях до сих является одной из крупнейших эпидемией в мире. По сообщению исследовательского центра компании Group-IB, в России атаке подверглись компьютерные системы "Роснефти", "Башнефти", "Евраза", российских офисов компаний Mars, Mondeles и Nivea. На Украине вирусной атаке подверглись компьютеры "Киевэнерго", "Укрэнерго", "Ощадбанка" и концерна "Антонов".

И наступающий 2018-й этот тренд продолжит только уже в чуть новом ключе – вместо шифровальщиков вымогающих деньги в обиход войдут вредонсосы скрытно использующие вычислительные мощности жертвы для веб-майнинга криптовалюты.

### Взлет криптовалюты и вредоносный майнинг

По сравнению с прошлым годом курс биткойна вырос в 15 раз и к концу года еще может легко побить этот рекорд. А капитализация платформы для умных контрактов Ethereum выросла вообще в 48 раз!

Если говорить прямо, то криптовалюты за текущий год оказали просто невероятное влияние на мировую экономику и уже существенным образом изменили рынок венчурных инвестиций. К примеру, объем привлеченных суммарных средств через ICO в 2017 году составил аж $3,5 млрд, тогда как традиционный IPO, имеет показатель чуть больше $1 млрд. Как вам такая разница?

И,конечно же логично, что с ростом этих новых технологий и ИТ-площадок связано появление и новых угроз и уязвимостей. Во-первых, это простор для разнообразных классических атак, как то создания фишинговых сайтов, взлома

web-ресурсов и подмены (мошенничества) биткойн-кошелька. По статистике предоставленной ЛК, по итогам года $300 млн, то есть фактически десятая часть средств, привлеченных через ICO, была украдена преступниками.

И это пока что не все новости! В связи с безумным распространением майнинга криптовалюты появились новые атаки, в частности скрытый майнинг, как с помощью инфицирования малварью и даже скриптинга в браузере так и взломе web-ресурсов с целью создания ботнет-сетей отдающий свои вычислительные мощности злоумышленникам.

## Malware на Android и iOS

По информации из отчета ЛК, в третей половине 2017 года резко возросло количество пользователей, атакованных мобильным банковским трояном Asacub. В июле текущего года количество жертв трояна выросло почти втрое, составив порядка 29 тыс. Также исследователи обнаружили новую модификацию мобильного трояна Svpeng, способного считывать введенный пользователем текст, отправлять SMS-сообщения и препятствовать своему удалению.

В этом же отчете также говорится о расширении списка мобильных приложений, атакуемых банковским трояном FakeToken. По мимо традиционного набора с фишинговыми страницами в сферу новых модификаций зловреда интересов вошли приложения для вызова такси, заказа авиабилетов и бронирования номеров в гостиницах. Основная цель трояна – сбор данных банковской карты пользователя.

В 2017 году по мимо всего прочего наблюдается и рост активности троянов, похищающих деньги пользователей посредством подписок. Так вредоносное ПО может нажимать кнопки на данных сайтах, используя специальные JS-файлы, таким образом осуществляя оплату неких услуг втайне от пользователя.

В TOP 10 банковских троянов, вошли Trojan-Spy..Zbot, Nymaim, Neurevt и Caphaw.

## Эксплоиты

В течении всего 2017 года продолжился рост количества атак на пользователей с использованием вредоносных офисных документов.

Несмотря на появление двух новых уязвимостей для пакета Microsoft Office, CVE-2017-8570 и CVE-2017-8759, злоумышленники продолжают эксплуатировать CVE-2017-0199 – найденную в марте 2017 года логическую уязвимость в обработке NTA-объектов.Суммарно доля эксплойтов для Microsoft Office составила в третьем квартале 27,80%.

В октябре обнаружили новый эксплойт для уязвимости нулевого дня в Adobe Flash, который доставлялся через документ Microsoft Office и использовался «в дикой среде» против наших клиентов. Мы уверены, что эта атака связана с группировкой, которую мы знаем под именем BlackOasis.

В третьем квартале не было крупных сетевых атак (таких как WannaCry или ExPetr) с использованием уязвимостей, исправленных в обновлении MS17-010.

Публикация дампа кода группировкой ShadowBrokers, в результате чего продвинутые эксплойты, якобы разработанные АНБ, попали в руки криминальных групп, которые иначе не получили бы доступа к коду такого высокого уровня.

## Вывод

Чем дальше продвигаются информационные технологии, тем больше сложностей по их использованию появляется. Технологии во многом упрощают нам жизни, но в тоже время
создают зависимости, на которые могут повлиять различные факторы с степенью опасности. Чем больше мы используем такие технологии как IoT, тем больше мы себя подвергаем потенциальным угрозам кибератак. Именно из-за подобных угроз на данный момент очень серьезно развивается такая отрасль технологий как информационная безопасность. Данная отрасль выходит на первый план в связи с ценностью информации в нашем обществе. Несмотря на то, что применяется огромное количество продуктов по защите, все же следует иметь представление о современных угрозах кибербезопасности и тенденциях, чтобы исключить неосторожные действия, которые могут привести к фатальным последствиям.

## Список литературы


1. Официальный сайт Cisco и Cisco Cibersecurity Annual Report 2017 https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=oemzzz000233&ccid=cc000160&oid=anrsc005679&ecid=8196

2. Официальный блог Microsoft и Security Intelligence Report 2017 https://news.microsoft.com/ru-ru/security-intelligence-report-2017-microsoft-predstavila-otchet-po-ugrozam-informatsionnoj-bezopasnosti/

3. Официальный сайт и блог Avast https://blog.avast.com/ru/prognoz-avast-osnovnye-kiberugrozy-2017-goda

4. Официальный сайт и блог Malwarebytes' Anti-Malware https://www.anti-malware.ru