УДК 004.056.5

А.В. Шевченко

Информационная и кибербезопасность: к эволюции проблемы

Аннотация:

В статье изложены ключевые идеи и проблемы информационной безопасности, способствовавшие развитию методов защиты информации, ставшие предтечей компьютерной информационной безопасности. Выделены значимые международные происшествия, способствовавшие повсеместному развитию кибербезопасности.

Ключевые слова: защита информации, информационные технологии, информационная безопасность, кибербезопасность, история криптографии.

Об авторе: Шевченко Алексей Валерьевич, Государственный университет «Дубна», аспирант, ассистент кафедры информационных технологий института системного анализа и управления; эл. почта: leviathan0909@gmail.com

Само понимание информационной безопасности неразрывно связано с понятием «информация» – существование первого немыслимо без второго, и по факту осознания человечеством ценности информации можно полагать начало формирования концепции информационной безопасности.

Наиболее ранними и яркими моментами в истории информационной безопасности традиционно отмечают первые упоминания о зашифрованных документах и описанных методах их кодирования. Показательным примером выступает шифр Цезаря, описанный в книге Гая Светония Транквилия «Жизнь двенадцати цезарей»: «Если у него было что-либо конфиденциальное для передачи, то он записывал это шифром, то есть так изменял порядок букв алфавита, что нельзя было разобрать ни одно слово. Если кто-либо хотел дешифровать его и понять его значение, то он должен был подставлять четвертую букву алфавита, а именно, D, для A, и так далее, с другими буквами» [4]. Конечно, это далеко не первое использование технологий защиты информации и сохранения

конфиденциальности через шифрование, но одно из наиболее ранних записанных и сохранившихся до наших дней.

Приведенный в качестве примера криптографический метод защиты информации был призван сохранить конфиденциальность передаваемых сведений при использовании общедоступного незащищенного канала передачи данных. Кроме свойства «конфиденциальность» в отношении информации принято обеспечивать еще такие свойства, как «целостность» и «доступность» [9]. Этот перечень свойств не является конечным и время от времени его дополняют частными характеристиками информации в зависимости от решаемых задач, например, «достоверность» или «неотказуемость».

По мере развития технологий связи методы обеспечения информационной безопасности усложнялись и становились более изощренными. Со временем чередование развития таких технологий и методов переросло в «гонку вооружений». Наиболее бурный рост за исторический период методы обработки информации и методы защиты информации переживали в XX в., который был ознаменован двумя мировыми войнами, неисчислимым количеством локальных конфликтов, началом холодной войны. Кроме огромного стимула к развитию систем связи подобные противостояния потребовали от участников столкновений разработки принципиально новых методов обеспечения сохранности свойств информации [11].

Описанный нами пример с шифром Цезаря примечателен еще и тем, что криптография в последующем своем развитии приведет человечество к реализации компьютерных технологий и переходу в цифровой век. Потребность в расшифровке немецких радиопереговоров, вычисление месторасположения подводных лодок, выявление траекторий их движения и планируемых мест нанесения ударов вынудило прибегнуть к проектированию электронно-механической машины для расшифровки кодов, успешно реализованной А. Тьюрингом. Впрочем, он не был пионером в этой области, поскольку стоит упомянуть М. А. Раевского и его команду, потратившую практически десять лет на взлом шифровальной системы Энигмы, чьи наработки были использованы А. Тьюрингом в расчетах.

Идеи, использованные при расшифровке Энигмы и развитые после Второй мировой войны, были реализованы А. Тьюрингом в 1946 г. в проекте первого британского компьютера – Автоматической вычислительной машины (ACE) [16]. Далее компьютерные технологии развивались по экспоненте. Стоит отметить выдающийся вклад Дж. фон

Неймана, определившего так называемую архитектуру фон Неймана, подразумевающую принцип хранения данных и инструкций в одной памяти вычислительной машины. Эта архитектура будет широко применяться в компьютерах и микропроцессорах, и останется актуальной более полувека.

Возвращаясь к криптографии, развитие концепции защиты информации неоднократно приводило к возникновению новых концептуальных математических моделей преобразования информации, призванных обеспечить требуемое состояние защищенности информации и компенсировать ранее выявленные уязвимости или неточности. Процесс не останавливался на всем периоде существования науки. Доклады в области безопасности и квантовых вычислений свидетельствуют, что век классической криптографии подходит к завершению, и постепенно мировое сообщество готовится к переходу в постквантовую криптографию [5; 15]. Ведущие университеты, занимающиеся вопросами защиты информации криптографическими методами, переходят к обсуждению собственной безопасности постквантовой технологии шифрования и ее устойчивости к определенным видам атак.

Потребность в разработке передовых вычислительных технологий и методов шифрования сохраняет свою актуальность благодаря несколькими современным факторам:

- постоянно возрастающей потребности в мощности вычислительных машин, подходящее к своему номинальному технологическому пределу в рамках существующей компьютерной архитектуры;
- достижениям в исследовании концептуально иных информационных структур, в частности, построенных на квантах и их запутанности;
- превосходству в скорости вычислений одних компьютерных архитектур над другими при решении базовых математических задач, на которые принято опираться при обеспечении информационной безопасности, что позволяет классифицировать новые квантовые технологии в том числе, как «наступательную технологию», способную дать тактическое преимущество в информационном пространстве.

Кроме приведенных видов деятельности в информационной безопасности принято выделять такие дисциплины, как защита интеллектуальной собственности, коммерческой тайны, частной жизни и персональных данных, служебной и государственной тайны, каналов передачи данных от перехвата и подмены, информации от неправомерного

доступа, защита от уничтожения и пр. Развитие компьютерных и информационных технологий продолжалось параллельно друг другу. Для понимания, что в конечном итоге определило состав кибербезопасности, следует разобрать два понятия:

1) Информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [14].

2) Компьютерные технологии – это обобщенное название технологий, отвечающих за хранение, передачу, обработку, защиту и воспроизведение информации с использованием компьютеров.

Из приведенных определений можно выделить несколько ключевых обстоятельств:

- компьютерная информационная безопасность – составная часть информационной безопасности;

- информационные технологии не обязательно включают в себя компьютерные технологии;

- компьютеры, будучи средством автоматизации (ускорения) информационных процессов, наследуют все риски информационной безопасности, существовавшие до их изобретения.

Говоря о компьютерных технологиях, следует упомянуть еще одного «отца компьютерного века», К. Шеннона. К его заслугам относят создание и развитие теории информации, стратегий для теории игр, идеи сжатия информации без потерь при распаковке [2; 13]. В своих работах Шеннон обосновал понятие энтропии и способствовал развитию современных сетей передачи данных. Развитие сетей передачи данных впоследствии способствовало появлению Интернета, что значительно ускорило проникновение компьютерных технологий в повседневную жизнь.

До начала 1990-х гг. компьютерные технологии оставались предметом изучения высокотехнологичных институтов, в том числе в силу дороговизны и крупных габаритов вычислительных машин. Переход из нишевой высокотехнологичной сферы в широкое обывательское потребление было обусловлено рядом факторов, среди которых следует выделить уменьшение габаритов вычислительных машин, упрощение процесса их эксплуатации, постоянную уменьшение форм-фактора и значительное удешевление устаревших компонентов, модульность структуры вычислительной машины, обусловившее возможность компоновки и модернизации для конечных пользователей,

появление приветливого и интуитивно понятного интерфейса базовых операционных сред, развитие сетей передачи данных и высоких языков программирования.

В то же время кажущаяся на первый взгляд техническая простота современных компьютеров скрывает под собой миллионы логических операций в секунду, выполняемых внутри чипов, гигабайты системных данных, неочевидные библиотеки, протоколы и драйвера. С одной стороны, современная компьютерная архитектура создана руками людей, с другой стороны даже ведущие производители операционных сред и физических компонентов отмечают, что уже не существует людей, способных самостоятельно в одиночку описать всю структуру работы современной вычислительной машины. Таким образом, по мере усложнения технологического оснащения компьютеров (логических и физических компонентов), вычислительные машины все больше становятся «черными ящиками» как для пользователей, так и для технических специалистов.

Эти же обстоятельства, описывающие постоянный рост и усложнение компьютерных систем, указывает в своих работах 2009 года Р. Лотуфо, отмечая, что сложность кода для конфигурационных опций операционных сред класса Linux постоянно возрастает. Это приводит к тому, что разработчики ядра Linux сталкиваются с трудностями при обслуживании этих конфигурационных опций особенно тогда, когда имеют дело с конфигурационными опциями, с несколькими зависимостями или с длинной цепочкой зависимостей [18]. Впоследствии более глубокая разработка кода программного продукта приводит к возникновению разрывов в зависимостях и качестве проработки отдельных модулей и последующему появлению незадекларированных возможностей или уязвимостей. Именно от этого факта возникает предпосылка для выделения в общем понятии информационной безопасности подвида компьютерной информационной безопасности.

Говоря о зарождении кибербезопасности как потребности в защите пространства и обработки данных, в первую очередь вспоминается червь Морриса – один из первых сетевых червей, распространявшихся через Интернет, написанный аспирантом Корнельского университета Р. Моррисом и запущенный 2 ноября 1988 г. в Массачусетском технологическом институте. Это был первый вирус, получивший значительное внимание в средствах массовой информации. Он также привел к первой судимости в США по статье о компьютерном мошенничестве 1986 г. Червь Морриса не был первой самовоспроизводящейся вирусной программой, но первой, приведшей к

осуждению ее автора и создавшей судебный прецедент, который подтолкнул законодателей многих стран вывести вопросы кибербезопасности из области этики и морали в законодательное регулирование [6].

Сами по себе компьютерный вирусы – это специально написанные небольшие по размерам программы, которые могут «приписывать» себя к другим программам (т.е. «заражать» их), а также выполнять различные нежелательные действия на компьютере. Все, что выполняет вирус, технически способен осуществить и любой пользователь системы. Отличием же выступает автономность вирусных программ, их способность к самораспространению и редупликации.

Вирусы не стали единственной причиной появления кибербезопасности. Компьютерная информационная безопасность качественно наследовала от классической (или общей) информационной безопасности. Следствием данного обстоятельства стали факты перехвата, подмены, блокирования информации в сетях передач данных. Благодаря развитию цифровых технологий по всему миру шпионаж и государственная разведка вышли на принципиально новый качественный уровень. Атаки на незащищенные средства и каналы передачи данных привели к закономерной необходимости построения систем (средств) защиты информации и развития технологий компьютерного шифрования.

Огромное влияние на развитие компьютерной информационной безопасности оказал ряд крупных событий, произошедших в период бурного роста информационных технологий. Так, к наиболее ярким вехам в истории человечества, предшествующим цифровой эпохе, приведшим к формированию современной парадигмы цифровой информационной безопасности, стоит отнести:

1. Конец 1980-х и начало 1990-х гг.: появление компьютерных вирусов и вредоносных программ. Неочевидность выполнения множества технических операций, выполняемых системой в процессе своего функционирования, оставило некоторое пространство для маневра злоумышленников и их автоматизированных инструментов.

Идея компьютерных вирусов впервые обсуждалась в серии лекций математика Дж. фон Неймана в конце 1940-х гг.; в 1966 г. вышла его монография «Теория самовоспроизводящихся автоматов» – по сути, это мысленный эксперимент, рассматривающий возможность существования «механического» организма – например,

компьютерного кода, который бы повреждал машины, создавал собственные копии и заражал новые машины аналогично тому, как это делает биологический вирус [8; 19].

Появление таких программ как Creeper и Rabbit, а также червя Морриса, о котором упоминалось ранее, мотивировали сообщество задуматься о разработке антивирусного программного обеспечения. Дальнейшее развитие идей вирусов еще неоднократно совершит переворот в системе защиты информации.

2. Вопрос конфиденциальности банковских данных, передаваемых в открытых сетях, не остался без внимания технических сотрудников и в 1994 году был представлен протокол SSL (Secure Sockets Layer) [21]. Netscape представила SSL, обеспечивающую зашифрованную связь между веб-браузерами и серверами и закладывающую основу для безопасных онлайн-транзакций. В дальнейшем данная технология защиты информации была призвана для защиты практически всей хоть сколько-то значимой информации в сетях передачи данных. В частности, протокол SSL используется для защиты от перехвата информации на популярных веб-сайтах, которые собирают персональные данные и используют онлайн-платежи.

3. Следующим значимым событием стала *реализация* Pretty Good Privacy (PGP) в 1996 году [20]. PGP, программное обеспечение для шифрования электронной почты и цифровой подписи, стало общедоступным, что обеспечило безопасную связь через Интернет.

4. Важную роль сыграло создание независимой международной Инженерной группы Интернета (IETF) в 1998 году для разработки и продвижения добровольных интернет-стандартов, включая протоколы безопасности. Сегодня в задачи IETF входит:

- идентификация проблем и предложение решений в технических аспектах организации Интернета;

- разработка спецификаций, стандартов и соглашений по общим архитектурным принципам протоколов Интернета;

- вынесение рекомендаций относительно стандартизации протоколов на рассмотрение Internet Engineering Steering Group (IESG);

- содействие широкому распространению технологий и стандартов, разрабатываемых в Internet Research Task Force (IRTF);

- организация дискуссии для обмена информации в сообществе Интернета между учеными, разработчиками, пользователями, производителями оборудования и услуг, сетевыми администраторами и т. д.

5. Масштабные распределенные атаки типа «отказ в обслуживании» (DDoS), участившиеся в 1999 г., привели к повышенному вниманию к сетевой безопасности. Следствием появления такого рода атак стало повышение требования к отказоустойчивости сетевого оборудования, появление специализированных протоколов безопасности и методов противодействия нарушению доступности сетевых ресурсов. Спустя 20 лет DDoS-атаки продолжаются качественно увеличиваться и в настоящее время сохраняют уверенную позицию в арсенале злоумышленников, атакующих слабозащищенные сетевые ресурсы.

Последствия от такого рода атак могут оказаться самыми разнообразными:

- полная или частичная остановка бизнес-процессов. Сейчас если не все, то большинство процессов в компаниях зависят от работы сети. Атака может сделать недоступными сервисы и сайты – перегрузить серверы или снизить пропускную способность соединения;

- ущерб деловой репутации. Актуально как для интернет-магазинов, так и для компаний, которые гарантируют доступность сервисов 24/7. И это очень серьезная проблема – по сведениям «Лаборатории Касперского» 23% компаний считают главной опасностью для бизнеса именно репутационный ущерб;

- снижение уровня ИБ. У любых инструментов ИТ-безопасности есть предел по количеству обрабатываемых запросов в секунду. При массированной DDoS-атаке часть ложных запросов проконтролировать не получится, что приведет к возникновению критических уязвимостей. Под прикрытием DDoS-атаки хакеры могут внедрить в систему вирусы-шифровальщики или получить доступ к корпоративной информации;

- технические трудности, связанные с необходимостью разворачивать резервные системы;

- дополнительные расходы. Отражение DDoS-атак, как и восстановление системы и сервисов после них, требует дополнительных расходов [3].

6. Террористические события 11 сентября 2001 г. в Нью-Йорке привели к созданию Патриотического акта США. Он был принят в ответ на теракты, расширив полномочия правительства по наблюдению и сбору данных.

Слежка, осуществляемая США, велась в планетарном масштабе, и несмотря на утечки и раскрытие информации, организованное в 2013 г. Э. Сноуденом, не прекращаются по настоящее время. О методах, применяемых АНБ, Сноуден рассказал в своей автобиографической книге, среди них – взломы смартфонов, домашних компьютеров и ноутбуков, слежка через социальные сети и уязвимости приложений, использование полученной информации не только для защиты, но и нападения на население собственной страны и игр на политической арене [12].

7. Широкое внедрение Wi-Fi и рост проблем с безопасностью беспроводных сетей ознаменовали 2004 г. С ростом использования Wi-Fi безопасность беспроводной сети стала серьезной проблемой, что привело к разработке протокола Wi-Fi Protected Access (WPA), а затем и WPA2. Вопросы безопасности беспроводных технологий на этом не закончились. По-прежнему остаются актуальными возможности перехвата сессий и расшифровки трафика на лету [7]. Тут беспроводные технологии никак не выпадают из концепции эволюции информационных технологий и связанных с ними методами атак злоумышленников.

8. Уже к 2008 г. понимание объема потенциального ущерба и общей стратегической значимости от реализации кибератак привело к появлению в ряде государств регулярных кибервойск и самоорганизующихся групп хакеров. Существование и деятельность таких группировок и подразделений привели к возникновению новой классификации угроз – усовершенствованные постоянные угрозы, Advanced Persistent Threats (APT) [22]. Целями деятельности APT-группировок зачастую становятся страны (группы стран), секторы промышленности и услуг и пр.

9. Примером деятельности APT-группировки выступает атака вредоносного программного обеспечения Stuxnet в 2010 г., направленная на иранскую ядерную программу. Результатом атаки стало замедление ее развития на несколько лет за счет диверсии на производстве [10]. Уникальность же самого происшествия заключается в том обстоятельстве, что результат превзошел ожидания и показал мировому сообществу эффективность кибероружия в деле.

10. В 2014 г. обнаружена ошибка Heartbleed – серьезная уязвимость в OpenSSL, которая затронула большое количество веб-сайтов и вызвала всеобщее беспокойство по поводу безопасности в Интернете [17]. Кроме объективного несовершенства технологии, подвергающего риску утечки конфиденциальную информацию, хранящуюся на сервере,

Heartbleed обратил внимание информационного сообщества на то, что уязвимости существуют повсеместно, даже в технологиях, кажущихся надежными.

11. Очередной виток эскалации киберугроз произошел в 2016 г. и был связан с многочисленным применением программ-вымогателей. Среди прочих ярко отметились атаки вирусов-шифровальщиков WannaCry и NotPetya в 2017 г., что еще больше подчеркнули необходимость повышения безопасности. Одним из наиболее значимых последствий по результатам массированного применения вирусов-шифровальщиков стала увеличение числа смертей пациентов вследствие не оказанной своевременно помощи [1].

12. В 2020 г. осуществлена кибератака на программное обеспечение Orion компании SolarWinds. Это была сложная атака на цепочку поставок, затронувшая несколько государственных учреждений и частных организаций США, что продемонстрировало необходимость повышения безопасности цепочки поставок. В процессе злоумышленники получили доступ к сетям как минимум 200 компаний и ведомств по всему миру. Точное число пострадавших компаний до конца не установлено. В частности, среди жертв упоминаются Cisco, Mimecast, Palo Alto Networks, Fidelis Cybersecurity, Microsoft. В результате атаки злоумышленники получили доступ к внутренней корпоративной документации.

Большое число инцидентов информационной безопасности, обусловленное цифровизацией многих развитых и развивающихся стран, стимулировало появление спроса на кибербезопасность. Современное общество столкнулось с популяризацией злонамеренной хакерской активности, вышедшей преимущественно из молодежного андеграунда, благодаря доступности цифровых технологий и низкой защищенности информационных активов. Проявления хактивизма, APT-атак, а также потребность в стабилизации бизнес-моделей, целиком зависящих от информационных и компьютерных технологий, привели к формированию на рынке труда запросов на технических специалистов по обеспечении кибербезопасности.

Общество хакеров разделилось на «черных», использующих свои навыки и знания в деструктивных целях, и «белых», преследующих диаметрально противоположные цели – обеспечение безопасности информационных ресурсов и процессов. Таким образом был осуществлен выход в новую парадигму обеспечения информационной безопасности в компьютерных системах: с одной стороны, ведется постоянная разработка техник нарушения состояний информационной безопасности в компьютерных системах, с другой

- поиск способов защиты. Реализованная концепция атаки-защиты нашло свое отражение в образовательных и соревновательных дисциплинах. Активно начало развиваться движение CTF-мероприятий (от «capture the flag»), начат переход к концепции комплексности информационной безопасности цифровых инфраструктур и кибериммунной безопасности, частные компании стали объявлять денежные награды за выявление и информирование о выявленных уязвимостях в их программных продуктах.

Стоит отметить, что переход от частных образовательных задач к олимпиадному соревнованию в кибербезопасности произошел буквально за 4-5 лет. Ветвление и развитие подходов к соревновательной дисциплине создало такие форматы состязаний, как CTF (attack/defense), CTF (jeopardy), Hack-quest, виртуальные лабораторные пространства (HTB, THM, Codeby.ctf), стенды виртуальных инфраструктур организаций (pentestit.lab) и даже городских инфраструктур (PhD Standoff 365). Обилие практики с необычными и нестандартными подходами для нарушения состояния защищенности и поиска полезных данных вывели кибербезопасность в самостоятельную образовательно-соревновательную дисциплину, в которой теперь могут специализироваться как разработчики цифровых инфраструктур, так и специалисты по информационной безопасности.

Реализация программ bugbounty (оплата за найденные уязвимости), как в индивидуальных политиках деятельности организации, так и объявление программ на открытых интернет-площадках привлекло множество молодых независимых энтузиастов к изучению технологий защиты и нападения в компьютерных технологиях, и благодаря открытой и свободной конкуренции позволило поднять общий уровень информационной безопасности ресурсов, публикуемых в сетях Интернет, на более высокий уровень.

Современная скорость развития информационных технологий, в том числе компьютерных, не позволяет оставаться информационной безопасности на одном месте дольше нескольких лет. Стоит лишь перейти новой технологии в массовое потребление, и она сразу же подвергается комплексному анализу на уязвимость. Определенно, за последние десятилетия обратная связь разработчиков новых технологий и потребителей значительно улучшилось, что позволяет более оперативно закрывать недостатки систем обновлениями компонентов или переходить на новую более качественную структуру. Однако это обстоятельство не спасает от «спящих» уязвимостей с чуть более сложной структурой реализации.

Сегодня процесс разработки кибериммунитета как концепции выглядит вполне логичным ответом на потребность в качественном управлении рисками. Необходимость глубокой экспертной оценки этих рисков и принятие оперативных компенсирующих решений подталкивают специалистов по защите информации к внедрению систем искусственного интеллекта. Такие решения, как поведенческий анализ, в конечном итоге должны снизить влияние человеческого фактора на общую безопасность.

Библиографический список:

1. Атаки шифровальщиков на больницы: последствия [Электронный ресурс] // Системы информационной безопасности. Блог. Режим доступа: https://is-systems.org/blog_article/11632986448 (дата обращения: 29.04.2023).

2. Венец В. Памяти Клода Шеннона // Информационные процессы. 2001. Т. 1, № 1. С. 99-100.

3. Все, что вы хотели знать о DDoS-атаках [Электронный ресурс] // Softline. Режим доступа: https://slddigital.com/article/vse-chto-vy-hoteli-znat-o-ddos-atakah/ (дата обращения: 25.04.2023).

4. Гай Светоний Транквилл. Жизнь двенадцати цезарей = De vita XII caesarvm. М.: Издательство «Наука» 1964. 374 с.

5. Квантовые вычисления представляют угрозу кибербезопасности. [Электронный ресурс] // SecurityLab. Режим доступа: https://www.securitylab.ru/news/537183.php (дата обращения: 25.03.2023).

6. Климентьев К. Е. Компьютерные вирусы и антивирусы: взгляд программиста. М.: ДМК Пресс, 2013. 656 с.

7. Кочуков А. Как провести перехват и скрытый анализ WiFi трафика без подключения к роутеру [Электронный ресурс] // Networkguru Безопасность. Режим доступа: https://networkguru.ru/perekhvat-i-analiz-wifi-trafika/ (дата обращения: 25.04.2023).

8. Краткая история компьютерных вирусов, и что сулит нам будущее [Электронный ресурс] // Kaspersky. Режим доступа: https://www.kaspersky.ru/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds (дата обращения: 30.03.2023).

9. Лукацкий А. Триада «конфиденциальность, целостность, доступность»: откуда она? [Электронный ресурс] // SecurityLab. Режим доступа:

https://www.securitylab.ru/blog/personal/Business_without_danger/24456.php (дата обращения: 30.03.2023).

10. Потапова А. В. Вирус Stuxnet – оружие нового поколения // Вестник магистратуры. 2014. Т. 1, № 3 (30). С. 10-12.

11. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. М.: Гелиос АРВ, 2005. 408 с.

12. Сноуден Э. Личное дело / ред. Логинова Я. В. М.: Издательство Эксмо, 2019. 416 с.

13. Тростников В. Н. Человек и информация. М.: Наука, 1970. 188 с.

14. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // «КонсультантПлюс». Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 28.06.2023).

15. Cheon J. Post-Quantum Cryptography / J. Cheon, T. Johansson // Heidelberg: Springer Cham, 2022. 523 p.

16. Copeland B. Alan Turing's Automatic Computing Engine. Oxford: Oxford University Press, 2005. 558 p.

17. Half a million widely trusted websites vulnerable to Heartbleed bug [Electronic resource] // Netcraft news. Archives. Available at: https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html (accessed date: 28.04.2023).

18. Lotufo R. On the complexity of maintaining the linux kernel configuration // Technical Report, Electrical and Computer Engineering, 2009. 17 p.

19. Neumann J. Theory of self-reproduction automata. London: University of Illinois Press 1966. Pp. 64-87.

20. OpenPGP Message Format [Electronic resouce] // RFC 4880. Network Working Group. Available at: https://datatracker.ietf.org/doc/html/rfc4880 (accessed date: 24.04.2023).

21. Secure Sockets Layer и Transport Layer Security [Electronic resource] // IBM. Available at: https://www.ibm.com/docs/ru/i/7.1?topic=concepts-secure-sockets-layer-transport-layer-security (accessed date: 14.04.2023).

22. The Advanced Persistent Threat [Electronic resource] // Internet Security Alliance. Available at: http://isalliance.org/publications/2013-06-06-ISA_APT_Paper-

Practical_Controls_for_SMBs.pdf (accessed date: 25.04.2023).

Shevchenko A.V. **Information and cybersecurity: towards the evolution of the problem**

The article outlines the key ideas and issues of information security that contributed to the development of information security methods and became the precursor of computer information security as a type of activity. Highlighting significant international incidents that contributed to the widespread development of cybersecurity.

Keywords: information security, information technology, cybersecurity, history of cryptography.