

Ю. Э. Голодков, Е. Ю. Ларионова,
Восточно-Сибирский институт МВД России, г. Иркутск

СОВРЕМЕННЫЕ ПОДХОДЫ К ФОРМИРОВАНИЮ КОМПЕТЕНЦИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ ВУЗОВ МВД РОССИИ

Аннотация

В статье рассматриваются вопросы формирования компетенций выпускников в области информационной безопасности и защиты информации, необходимых для успешной деятельности в правоохранительной системе России. Показано, что в связи с высокой скоростью развития информационных технологий для качественной подготовки сотрудников органов внутренних дел необходимо существенно расширять их профессиональный кругозор в области защиты информации.

Ключевые слова: информационные технологии, информационная безопасность, профессиональные компетенции, технологии квантовой связи.

Информационные технологии — один из наиболее важных факторов, влияющих на развитие современного общества в XXI веке. Достижения науки и техники, к сожалению, с успехом используются и в преступных целях. Хакеры в области финансового мошенничества стали использовать искусственный интеллект, вирусы стали значительно более опасными и самообучаемыми при прохождении различных систем защиты. Сбербанк России ожидает, что количество кибератак, нацеленных на кражу средств клиентов банка, увеличится к 2020 году не менее чем в 10 раз [8]. Действия мошенников не ограничиваются финансовыми учреждениями. Например, глобальная атака вируса-вымогателя 27 июня 2017 года поразила ИТ-системы компаний в нескольких странах мира, в большей мере атаке подверглись компьютеры нефтяных, энергетических, телекоммуникационных и фармацевтических компаний, а также госорганов [3]. В США хакеры смогли получить доступ к компьютерной сети как минимум одной американской атомной электростанции, взлом затронул важные операционные данные компьютерной системы пользователей. Вирусные атаки были

нацелены на энергетический сектор с целью проведения кибершпионажа и возможного нарушения работы энергетических сетей [11].

Кибератакам с целью шпионажа непрерывно подвергаются и компьютерные сети МВД России [7]. Так, в мае 2017 года была зафиксирована вирусная атака на сеть компьютеров ИСОД МВД России — единой системы информационно-аналитического обеспечения деятельности. Все подключенные к системе персональные компьютеры под управлением операционной системы Windows были заблокированы, однако утечки служебной информации с информационных ресурсов удалось избежать. Отголоски хакерской атаки почувствовали во многих территориальных подразделениях правоохранительной системы России — отсутствовал доступ к базам данных, наблюдались перебои с телефонной связью. Серверные ресурсы ведомства не подверглись заражению во многом благодаря использованию операционных систем и отечественных серверов с российским процессором «Эльбрус».

Всего, по данным «Лаборатории Касперского», за короткий период в 2017 году было зафиксировано

Контактная информация

Голодков Юрий Эдуардович, канд. тех. наук, доцент, начальник кафедры информационно-правовых дисциплин Восточно-Сибирского института МВД России, г. Иркутск; *адрес:* 664074, г. Иркутск, ул. Лермонтова, д. 110; *телефон:* (3952) 41-11-17; *e-mail:* yrg27@mail.ru

Ларионова Елена Юрьевна, доктор хим. наук, доцент, профессор кафедры информационно-правовых дисциплин Восточно-Сибирского института МВД России, г. Иркутск; *адрес:* 664074, г. Иркутск, ул. Лермонтова, д. 110; *телефон:* (3952) 41-11-17; *e-mail:* lari888@mail.ru

Yu. E. Golodkov, E. Yu. Larionova,
East Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk

MODERN APPROACHES TO THE DEVELOPMENT OF TRAINEES' COMPETENCIES IN THE FIELD OF INFORMATION SECURITY IN THE EDUCATIONAL INSTITUTIONS OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Abstract

The article examines some issues concerning the development of graduates' competencies in the field of information security and data protection essential for the success of law enforcement in Russia. It is shown that provided by advances in information technologies for the quality training of law enforcement officers it is necessary to significantly expand their professional visibility in the field of information security.

Keywords: information technologies, information security, professional competencies, quantum communication technologies.

около 45 тыс. попыток хакеров атаковать компьютеры по всему миру с помощью вируса-шифровальщика WannaCry, который шифрует файлы пользователя, изменяет их расширение и требует купить специальный расшифровщик за биткойны, в противном случае файлы будут удалены [5].

Кроме того, отношение числа правонарушений, совершаемых при помощи информационных технологий, к правонарушениям, совершаемым традиционными способами, стремительно возрастает.

Будущая работа выпускников образовательных организаций Министерства внутренних дел Российской Федерации сопряжена с активным использованием средств информационно-телекоммуникационных технологий. И от грамотного использования информационных ресурсов, наличия у сотрудников соответствующих знаний, умений и навыков в области информационных технологий зависит в целом информационная безопасность органов внутренних дел. Системе высшего образования в этом случае отводится важная роль в формировании компетенций выпускников в области информационной безопасности и защиты информации, необходимых для успешной деятельности в правоохранительной системе России.

В соответствии с требованиями федерального государственного образовательного стандарта высшего образования на примере направления подготовки 40.05.01 «Правовое обеспечение национальной безопасности» [9] изучение вопросов информационной безопасности и защиты информации предполагает освоение таких компетенций, как:

- способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12);
- способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-16).

Освоение этих компетенций предполагает формирование основных знаний, умений и навыков курсантов и слушателей вузов МВД России. Обучающийся должен при этом знать нормативные правовые акты в области защиты информации и противодействия техническим разведкам, основные понятия и угрозы информационной безопасности ОВД, основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности. Полученные умения должны позволить выпускнику:

- ориентироваться в программно-технических, правовых и организационных методах защиты информации;
- использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты защищаемой информации;
- оценивать опасность, связанную с угрозами несанкционированного доступа к информации,

намеренной модификации данных и утраты служебной информации;

- формулировать проблемы и задачи для их решения специалистами служб безопасности и защиты информации.

При этом предполагается, что выпускник будет владеть:

- навыками безопасного использования вычислительной техники при решении служебных задач;
- современными общими способами обеспечения информационной безопасности;
- базовыми программно-аппаратными методами защиты информации [1].

Перечисленные знания, умения и навыки выпускников в области информационной безопасности и защиты информации представлены в общем идеализированном виде, их полное освоение возможно только в процессе дальнейшей профессиональной деятельности в определенной области. Понимание сущности и значения информации в деятельности органов внутренних дел, знание опасностей и угроз, возникающих в процессе профессиональной деятельности, — это только некоторые вопросы по соблюдению требований информационной безопасности и защиты информации. Задача поддержания информационной культуры сотрудников органов внутренних дел должна решаться не только в период обучения в образовательных организациях и в результате прохождения плановых курсов повышения квалификации, но и в процессе самообразования. Одной из стратегических целей обеспечения информационной безопасности является формирование у сотрудников органов внутренних дел культуры личной информационной безопасности. Особый режим профессиональной деятельности и возможность допуска к сведениям конфиденциального характера или служебной информации ограниченного пользования требуют от сотрудника органа внутренних дел соблюдения этических и правовых норм использования информационно-компьютерных технологий.

На общепринятом системном представлении выделяются следующие уровни информационной безопасности:

- нормативно-правовой;
- организационный;
- процедурный;
- программно-технический [6].

Формирование компетенций в области информационной безопасности при изучении таких дисциплин, как «Основы информационной безопасности» и «Информатика и информационные технологии в профессиональной деятельности», касается в основном *нормативно-правового и организационного* уровня информационной безопасности.

Для формирования *процедурного и программно-технического* уровней информационной безопасности требуются более глубокие знания.

По нашему мнению, для достижения полноценной отдачи при изучении базовых указанных учебных дисциплин требуется расширить перечень необходимых компетенций, формирующих знания, умения и навыки обучающихся в области информационной безопасности и защиты информации.

В частности, чрезвычайно важным является способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве. Для формирования компетенций в области информационной безопасности обучающимся крайне не хватает знаний в области математики, физики и даже химии. Школьного курса математики явно недостаточно для изучения даже только основ криптографических методов защиты информации. Изучение классических основ защиты информации, связанных с такими базовыми понятиями, как модель криптосистемы с открытым ключом, открытое распределение ключей, алгоритм Диффи-Хеллмана, криптосистема RSA, электронная подпись, хэш-функции и т. д., становится чрезвычайно затруднительным для курсантов и слушателей.

В настоящее время тотального использования информационных технологий во всех областях общественной жизни следует больше уделять внимания формированию компетенций в области информационной безопасности и защиты информации. В связи с этим считаем целесообразным для профессиональной подготовки сотрудников органов внутренних дел не ограничиваться изучением дисциплины «Основы информационной безопасности», а заменить ее на учебную дисциплину «Информационная безопасность и защита информации», в которой предусмотреть достаточное количество зачетных единиц. В настоящее время для изучения учебной дисциплины «Основы информационной безопасности» отведено две зачетных единицы, и качественное освоение даже перечисленных компетенций специалистами направления подготовки 40.05.01 «Правовое обеспечение национальной безопасности» не представляется возможным.

Авторы статьи [2] отмечают, что для формирования компетенций в области информационной безопасности необходимо выделить ее *инвариантную* (системообразующую) и *вариативную* (направленную на решение конкретных профессиональных задач) составляющие. Для формирования системного целостного представления об информационной безопасности необходимо включать в учебные планы дисциплину «Информационная безопасность и защита информации».

Системы информационной безопасности постоянно совершенствуются, и курсанты, приступающие к изучению информационных технологий на первом курсе, по окончании обучения через пять лет практически обладают уже устаревшими знаниями и умениями в этой стремительно развивающейся сфере. По нашему мнению, *образовательная программа должна предусматривать возможность изучения информационных технологий применительно к практическому использованию в профессиональной деятельности на протяжении всего периода обучения.*

На текущий момент одним из решающих факторов обеспечения информационной безопасности в деятельности государственных органов является разработка и внедрение отечественного программного и аппаратного обеспечения. Об этом свидетельствуют факты вирусостойчивой работы ведомственных компьютерных ресурсов на основе использования

операционных систем и отечественных серверов с российским процессором «Эльбрус».

«К 2024 году в России в соответствии с проектом государственной программы “Цифровая экономика” должны появиться как минимум десять высокотехнологичных и конкурентоспособных на глобальном рынке предприятий в сфере высоких технологий (большие данные, нейротехнологии, квантовые технологии, промышленный интернет, робототехника, виртуальная и дополненная реальности, системы распределенного реестра и др.), десять “отраслевых/индустриальных цифровых платформ для основных отраслей экономики”» [12] (в том числе для цифрового здравоохранения, цифрового образования и «умного» безопасного города).

Большое внимание в программе «Цифровая экономика» уделено российскому софту и оборудованию. К концу срока реализации программы доля иностранного компьютерного, серверного и телекоммуникационного оборудования, закупаемого госорганами, должна снизиться до 50 %, а программного обеспечения — до 10 %. В проекте говорится, что производители отечественного компьютерного, серверного и телекоммуникационного оборудования должны получить преференции при поставках госорганам уже к концу 2018 года. Частично использовать российское оборудование намерены и в создаваемой распределенной системе центров обработки данных (ЦОД), которая должна появиться к концу 2020 года и обеспечить обработку всех данных, формируемых гражданами и организациями на территории России. К 2024 году в каждом из федеральных округов страны должно появиться по одному опорному ЦОДу. Координацией системы и обеспечением ее безопасности займется ситуационный центр мониторинга и управления инфраструктурой хранения и обработки данных.

Информационная среда Министерства внутренних дел становится более открытой для общества за исключением, естественно, профессиональных задач. В соответствии со статьей 1 Федерального закона от 7 февраля 2011 года № 3-ФЗ «О полиции» «полиция предназначена для защиты жизни, здоровья, прав и свобод граждан Российской Федерации, иностранных граждан, лиц без гражданства (далее также — граждане; лица), для противодействия преступности, охраны общественного порядка, собственности и для обеспечения общественной безопасности» [10, с. 1]. Эффективной формой выполнения этих задач является участие органов внутренних дел в реализации таких проектов, как «Безопасный город», и выпускникам образовательных организаций МВД России необходимо будет уверенно использовать последние разработки информационных технологий в соответствии с реализацией программы «Цифровая экономика».

Практически все вышеперечисленные системы безопасности обеспечиваются технологиями шифрования, которые способны защищать информацию от злоумышленников и посторонних лиц. Эту сложную проблему на текущий момент блестяще решили разработчики современных криптосистем. Однако сегодня возникает вопрос, не разрушат ли систему защиты, основанную на криптографических методах,

новые разработки в области информационных технологий, а именно, с одной стороны, лавинообразное увеличение производительности и быстродействия современных компьютеров, с другой — появление таких технологий, как квантовые вычисления и квантовая связь, которые предвещают революцию в области защиты информации.

Теоретической основой квантовых технологий являются принципы квантовой механики, примененные для обработки информации. В частности, принцип неопределенности Вернера Гейзенберга, согласно которому невозможно одновременно с одинаковой степенью точности измерить координаты и импульс частицы. Иначе говоря, чем точнее определены значения пространственных координат частицы, тем более неопределенным становится ее импульс. И наоборот, чем точнее определен импульс частицы, тем более неопределенным является ее пространственное положение [4]. То есть состояние или положение частицы можно определить только с некоторой долей вероятности. Второй принцип — квантовая суперпозиция или суперпозиция состояний. Если частица может иметь несколько состояний, то согласно этому принципу она находится одновременно во всех возможных состояниях. При этом процесс измерения состояния частицы приводит к изменению ее состояния.

Всем известно, что классический процессор ЭВМ оперирует в своих действиях бинарным кодом, представляющим два состояния (0, 1). Квантовые компьютеры оперируют кубитами или квантовыми битами. Кубит отличается от бита тем, что он представляет собой два состояния (0, 1), которые как бы перекрываются в разной пропорции.

Для лучшего понимания принципиального различия между классическим бистабильным элементом и кубитом проводят интересную аналогию. А именно сравнивают два пикселя, соответствующих классическому бистабильному элементу и кубиту. Классический пиксель может быть лишь черным или белым. Напротив, пиксель, соответствующий кубиту, может быть любого цвета или иметь любые цветовые оттенки, при этом он несет намного больше информации. Считают, что квантовые технологии приведут к предпосылкам для грандиозных научных открытий. В частности, они позволят радикально ускорить математические вычисления, в том числе осуществлять подбор криптографических ключей.

Возможно и построение на данных позициях систем информационной безопасности и защиты информации. И действительно, за последние двадцать пять лет появившаяся квантовая криптография прошла путь от теоретических исследований и доказательства основных теорий до коммерческих систем, использующих оптическое волокно для передачи на расстояние десятков километров [4].

Классическая криптография основана на математических методах, предполагающих теоретическую невозможность подбора текста закрытого ключа современными техническими средствами. Секретность квантовой криптографии базируется на квантовых явлениях, в частности, состояниях электронов в электрическом токе и фотонов в случае волоконно-оптической связи. В основе технологии квантовой

криптографии также лежит принцип Гейзенберга. Сегодня в квантовой криптографии выделяют два основных направления развития систем распределения ключей.

Первое направление основано на кодировании квантового состояния одиночной частицы и базируется на принципе невозможности различить абсолютно надежно два неортогональных квантовых состояния. Благодаря унитарности и линейности квантовой механики невозможно создать точную копию неизвестного квантового состояния без воздействия на исходное состояние.

Второе направление развития основано на эффекте квантового перепутывания (запутывания). Две квантово-механические системы, в том числе разделенные пространственно, могут находиться в состоянии корреляции, так что измерение выбранной величины, осуществляемое для одной из систем, определит результат измерения этой величины относительно другой [4].

Следовательно, используется принципиальная неопределенность поведения элементов квантовой системы, которая заключается в том, что невозможно измерить один параметр квантовой частицы, не исказив другой. Подслушивание, в форме попытки измерения взаимосвязанных параметров элементов квантовой системы, вносит в нее нарушения и разрушает исходные сигналы, таким образом, уровень шума становится сигналом активности перехватчика. Попытка злоумышленников похитить секретную информацию приводит к изменению ее содержания.

Устойчивость традиционных методов шифрования может быть легко нарушена с появлением более мощных квантовых компьютеров, способных математически раскрыть содержание секретного кода безопасности. Появление таких абсолютно новых вычислительных систем — это прорыв для науки, но и опасность для существующих принципов защиты информации. Расчеты по раскодированию любых самых сложных математических шифров, которые с применением традиционного компьютера могут занять тысячу лет, квантовый компьютер в состоянии выполнить мгновенно.

Таким образом, характерной чертой современной экономики являются заметные успехи в развитии наукоемких производств, в том числе информационных технологий. В современных условиях информация стала стратегическим ресурсом, и масштабы угроз, использующих информационные технологии, продолжают расти. Поэтому формирование профессиональных компетенций сотрудников правоохранительных органов в области информационной безопасности должно стать одной из первоочередных задач современной системы образования МВД России. Следовательно, для качественной подготовки сотрудников органов внутренних дел нельзя ограничиваться только изучением дисциплины «Основы информационной безопасности», профессиональный кругозор в области защиты информации необходимо существенно расширять, дополняя предварительным обеспечением понимания обучающимися не только нормативно-правовой базы, но и смысла физических процессов и принципов построения соответствующих алгоритмов.

Список использованных источников

1. Баранов С. А., Голодков Ю. Э., Демаков В. И., Кургалеева Е. Е. Основы информационной безопасности в органах внутренних дел: учебное пособие. Иркутск: ФГКОУ ВПО ВСИ МВД России, 2015.
2. Бушмелева Н. А., Разова Е. В. Формирование компетенций в области информационной безопасности в системе высшего педагогического образования // Концепт. 2017. Т. 2. <https://e-koncept.ru/2017/570106.htm>
3. Вирус-вымогатель атаковал IT-системы компаний. <https://ria.ru/world/20170627/1497409144.html>
4. Голубчиков Д. М., Румянцев К. Е. Квантовая криптография: принципы, протоколы, системы. <http://window.edu.ru/catalog/pdf2txt/801/58801/28663>
5. Ивашкина Д. «Лаборатория Касперского» зафиксировала 45 тысяч попыток кибератак // Комсомольская правда. 12 мая 2017 года. https://www.kp.ru/online/news/2743342/?utm_campaign=transit&utm_source=mirtesen&utm_medium=news&from=mirtesen
6. Курзаева Л. В., Чусавитина Г. Н. К вопросу формирования требований к компетенциям личности в об-

ласти информационной безопасности в системе высшего профессионального образования // Фундаментальные исследования. 2013. № 8. Ч. 5.

7. МВД России зафиксировало вирусную атаку // Известия. 12 мая 2017 года. <https://iz.ru/news/705164>

8. Президент Сбербанка прогнозирует бесконечную борьбу с хакерами // Информационное агентство «NewsTes». <http://newstes.ru/2017/12/14/prezident-sberbanka-prognoziruet-beskonechnuyu-borbu-s-hakerami.html>

9. ФГОС ВО по направлению подготовки 40.05.01 Правовое обеспечение национальной безопасности. <http://fgosvo.ru/uploadfiles/fgosvospec/400501.pdf>

10. Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 05.12.2017) «О полиции». <http://base.garant.ru/5763186>

11. Хакеры взломали компьютерные системы АЭС // Спутник/Новости. <https://news.sputnik.ru/internet/0f875148aafeld9a66ca5358d2363cfb349bfd46>

12. Цифра должна быть суверенной — Обзор СМИ. 3 июля 2017 года // Научно-исследовательский институт радио. <http://niir.ru/cifra-dolzha-byt-suverennoj-obzor-smi/>

НОВОСТИ

Gartner: в 2018 году мировой рынок средств безопасности вырастет на 8 %

По прогнозам аналитиков, мировой объем продаж средств информационной безопасности (средств управления доступом и идентичностью, защиты инфраструктуры, оборудования для сетевой безопасности, услуг, а также ПО потребительского класса) в 2018 году вырастет на 8 % по сравнению с 2017 годом и достигнет 96,3 млрд долл. Увеличение расходов на средства безопасности в значительной степени связано с недавними громкими случаями утечки данных из-за кибератак. Именно поэтому среди сегментов рынка быстрее других будут расти сегменты средств тестирования безопасно-

(По материалам международного компьютерного еженедельника «Computerworld Россия»)

Российские технологии детекции лиц и автомобилей перенесли на «Эльбрусы»

Российский разработчик систем распознавания и обработки изображений Smart Engines адаптировал часть своих решений под платформу «Эльбрус» и перешел на цикл, когда новые разработки сразу создаются под отечественные процессоры, т. е. не требуют последующего так называемого портирования. Некоторые из разработок были созданы специально под актуальные задачи российской полиции.

По словам представителя МЦСТ (компании — разработчика процессоров «Эльбрус» Максима Горшенева, ПО Smart Engines работает на персональной станции «Эльбрус 801-PC», а также на вычислительном комплексе «Эльбрус 101-PC», который может выполнять функции бортового вычислителя в автомобиле или располагаться на мачте с видеокамерой. Непосредственно софт распознавания поддерживает четырехядерные «Эльбрус-4С», восьмиядерные «Эльбрус-8С» и процессоры со встроенным видеоядром и поддержкой аппаратного ускорения 3D-графики «Эльбрус-1С+».

Компании МЦСТ и Smart Engines уже имели опыт сотрудничества, в частности, в проекте создания программно-аппаратного комплекса «Всеслав», назначением которого является сбор, обработка, индексирование и хранение персональных данных, полученных из различных источников: фото, видео, сканов документов и пр. Теперь список

ИТ-аутсорсинга и систем управления информацией о безопасности и событиями безопасности (SIEM). Сответствующие вложения также стимулируются новыми законами о защите данных. Дефицит специалистов, техническая сложность и характер угроз подталкивают компании к внедрению средств автоматизации и переходу на аутсорсинг. В 2018 году расходы на аутсорсинговые услуги в области безопасности вырастут в мире на 11 %, до 18,5 млрд долл., полагают аналитики, а к 2019 году их доля в корпоративных бюджетах информационной безопасности вырастет до 75 % с 63 % в 2016 году.

разработок с применением технологий обеих компаний пополнился решениями по идентификации лиц в потоке визуальных объектов, детекции транспорта в движении, панарамировании (склеивке в единую картинку группы фотографий), детекции сигналов светофоров, распознаванию удостоверений личности и номеров автомобилей.

Гендиректор Smart Engines Владимир Арлазаров пояснил, что детекция сигналов светофоров нужна для определения по видео, работает ли устройство в принципе (система вычлняет светофоры из множества других огней на трассе) и по нужному ли алгоритму. Что касается детекции транспорта в потоке, то в данном случае система на ходу (с борта автомобиля) распознает другие машины, движущиеся в попутном направлении, по визуальным признакам. Подобный детектор может использоваться в системах автоматического управления транспортом.

Технология определения положения транспортного средства в городе с видеокартинки, без ГЛОНАССА и GPS сличает картинку окружающей обстановки с камеры и сравнивает с сохраненной базой. Далее определяет, с какими картинками в базе наилучшее совпадение, и по координатам, сохраненным в базе, определяет координаты текущего местоположения.

(По материалам CNews)