Константин Саматов

Карьера в информационной безопасности

Константин Саматов

Карьера в информационной безопасности

«Издательские решения»

Саматов К. М.

Карьера в информационной безопасности / К. М. Саматов — «Издательские решения»,

ISBN 978-5-00-514195-8

Эта книга о карьере в информационной безопасности, о месте информационной безопасности в безопасности бизнеса и не только.Книга предназначена прежде всего для тех, кто начинает свой путь в информационной безопасности — обучается на соответствующих специальностях в средних и высших учебных заведениях.Книга может быть полезна руководителям и специалистам по работе с персоналом, т.к. в ней изложен опыт автора по адаптации работников в подразделении информационной безопасности.

ISBN 978-5-00-514195-8

Содержание

Карьера в информационной безопасности

Константин Михайлович Саматов

ISBN 978-5-0051-4195-8
Создано в интеллектуальной издательской системе Ridero

Предисловие. О чем и для кого эта книга?

Эта книга о карьере в информационной безопасности, о месте информационной безопасности в безопасности бизнеса, и не только. Книга предназначена, прежде всего, для тех, кто начинает свой путь в информационной безопасности – обучается на соответствующих специальностях в средних и высших учебных заведениях. Также книга может быть полезна руководителям и специалистам по работе с персоналом, т.к. в ней изложен опыт автора по адаптации работников в подразделении информационной безопасности, в том числе выпускников учебных заведений, не имеющих практического опыта.

Как возникла идея написания этой книги? Автор более 17 лет является практикующим специалистом в сфере безопасности и значительное количество времени уделял именно вопросам информационной безопасности. Много лет назад у него появилась мысль о том, что если бы в процессе обучения студентов принимали участие реальные практики и умели сочетать подачу теоретического материала со своим практическим опытом, то на выходе получались бы гораздо более квалифицированные и адаптированные к работе в реальном секторе экономики специалисты.

Поэтому, с 2014 года он начал заниматься реализацией этой идеи – преподавать, сначала в среднем специальном учебном заведении (колледже), затем в высшем (университете), совмещая преподавательскую деятельность с работой в подразделении информационной безопасности. Общаясь со студентами и затрагивая вопросы карьеры автору, нередко, приходилось наблюдать не совсем верное представление о выбранной профессии.

Помимо работы в учебных заведениях, большой пласт усилий автора был связан с подготовкой кадров непосредственно на рабочих местах – это были как студент последних курсов, так и окончившие учебные заведения юноши и девушки, начинающие свой путь в информационной безопасности.

Как следствие и возникла идея рассказать о том, что такое информационная безопасность, о карьере в данной сфере и дать некоторые рекомендации тем, кто ее выбрал: учащимся и выпускникам – как строить свою карьеру с нуля, а тем кто занимает руководящие посты – как не бояться брать людей без опыта и выращивать из них настоящих профессионалов.

Данная книга не является учебным пособием и не претендует на истину в последней инстанции, основная её цель – поделиться собственным опытом, не потратив много времени читателя, изложив его в сжатом виде.

Глава 1. Что такое информационная безопасность?

Не сильно углубляясь в теорию, можно определить **«информационную безопасность»**, как одно из направлений корпоративной безопасности (по сути, одну из составляющих), связанную с обеспечением состояния защищенности информации, т.е. таких ее свойств как конфиденциальность, целостность и доступность (рисунок 1).

В свою очередь **«корпоративная безопасность»** – комплекс мер, направленных на обеспечение информационной, инженерно-технической, экономической, кадровой и юридической безопасности организации, направленных на сохранение и обеспечение нормального осуществления всех процессов (деловых процессов) ее жизнедеятельности.

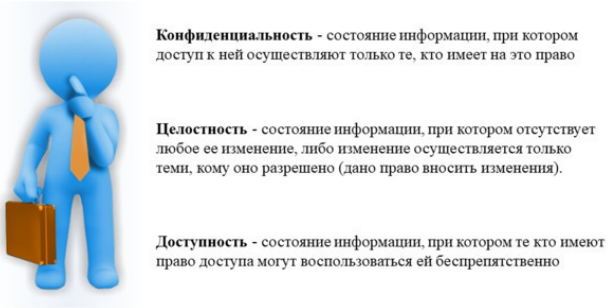

Рисунок 1. – Свойства информации

Таким образом, следует понимать (и это очень важно), что информационная безопасность является составной частью всей безопасности компании (элементом системы) и рассматривать ее изолированно, по мнению автора, не правильно. Информационная безопасность должна рассматриваться в контексте с другими элементами системы безопасности компании и наиболее тесно с кадровой безопасностью, инженерно-технической и юридической, а если брать тенденции последних лет, связанные с переходом активов компаний в электронный вид (т.н. «цифру»), то, пожалуй, еще и с экономической безопасностью.

Важно затронуть и еще одно понятие, тесно связанное с информационной безопасностью и, нередко, используемое в качестве синонима – это **«защита информации»**. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности и доступности информации. Иными словами, защита информации – это процесс, направленный на достижение состояния информационной безопасности.

Таким образом, синонимом понятия «защита информации» будет являться не безопасность информации (информационная безопасность), а «обеспечение информационной безопасности».

С точки зрения Российского права (ст. 16 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации») защита информации (обеспечение информационной безопасности) представляет собой обеспечение конфиденциальности, целостности и доступности путем принятия:

– правовых мер – разработка норм права направленных на регулирование отношений в сфере информационной безопасности;

– организационных мер – организация деловых процессов[1] обработки информации;

[1] Процесс – совокупность последовательных действий для достижения какого-либо результата (например, процесс ввода

– технических мер – применение технических средств для защиты информации и информационных активов[2].

По мнению автора, данная классификация может быть дополнена еще т.н. «морально-этическими мерами», заключающимися в работе с людьми (персоналом) и направленными на минимизацию совершения ошибок в процессах обработки информации, а также на недопущение умышленных действий, влекущих нарушение правил информационной безопасности.

Важность понимания указанной классификации вызвана следующим: очень часто, на практике, автору приходилось сталкиваться с мнением о том, что информационная безопасность – это деятельность, связанная исключительно с техническими аспектами защиты информации и информационных активов. На самом деле, на практике это совершенно не так.

Что же представляет собой информационная безопасность на практике?

информации, процесс обращения бумажных документов в организации, процесс допуска работника на территорию организации и т.п.).

[2] Информационный актив – информационный ресурс или средство обработки информации (например, база данных, архив бумажных документов, персональный компьютер, сервер и т.п.).

Глава 2. Информационная безопасность на практике

Опираясь на реалии рынка труда и текущие потребности предприятий и организации в специалистах, можно выделить следующие направления в информационной безопасности:

– *Организационно-правовая безопасность* – менеджерское направление обеспечения информационной безопасности, его представители обычно занимают такие должности как: «менеджер по информационной безопасности», «менеджер по методологии информационной безопасности», «аналитик», «эксперт по информационной безопасности», «руководитель подразделения (отдела, службы, управления) информационной безопасности». Основной функционал указанных специалистов связан с выстраиванием процессов безопасной обработки информации в организации и их совершенствованием, обеспечением соответствия требованиям внешнего (законы и подзаконные нормативно-правовые акты) и внутреннего (локальные нормативные акты) регулирования.

– *Техническая безопасность* – инженерное направление обеспечения информационной безопасности, его представители обычно занимают такие должности как: «техник по защите информации», «инженер по защите информации», «специалист по технической защите информации», «инженер-программист», «инженер-проектировщик», «инженер-архитектор» (систем информационной безопасности), «специалист по анализу защищенности компьютерных систем и сетей», «специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак», «технический эксперт». Основной функционал указанных специалистов связан с установкой и настройкой средств и систем защиты информации, обеспечением их бесперебойного функционирования.

– *Конкурентная разведка и управление репутацией компании.* Несмотря на то, что данное направление не относится к «классической» информационной безопасности, на практике, в большинстве случаев, руководитель компании видит указанный функционал именно в специалистах по информационной безопасности.

Остановимся на этих двух направлениях более подробно, чтобы показать их связь с информационной безопасностью.

Конкурентная разведка (англ. Competitive Intelligence) – сбор и обработка данных из различных источников, для выработки управленческих решений с целью повышения конкурентоспособности организации, проводимые в рамках закона и с соблюдением этических норм (в отличие от промышленного шпионажа)[3]. По сути, это особый вид информационно-аналитической работы, позволяющий собирать обширнейшую информацию о юридических и физических лицах без применения специфических методов оперативно-розыскной деятельности, являющихся исключительной прерогативой государственных правоохранительных органов и спецслужб. Именно поэтому, данный вид деятельности часто относят к сфере безопасности.

Другие часто встречающиеся названия конкурентной разведки – бизнес-разведка, деловая разведка, аналитическая разведка, маркетинговая разведка, коммерческая разведка.

Глобально конкурентную разведку можно поделить на два направления – OSINT и HUMINT:

– *OSINT (Open source intelligence)* – сбор информации из общедоступных источников, прежде всего СМИ и сети Интернет. При этом, при сборе информации очень часто используются различные способы и методы, характерные для мероприятий по анализу защищенности информационных систем, а сама процедура сбора информации из открытых источников обычно является одной из начальных стадий так называемого тестирования на проникновение

[3] https://ru.wikipedia.org/wiki/Конкурентная_разведка

(Penetration Test), в виду чего указанное направление деятельности и стали относить к информационной безопасности.

– *HUMINT (Human intelligence)* – сбор информации с использованием людей. По сути сбор информации от человека, в том числе с использованием методов социальной инженерии, которые широко используется при тестировании на проникновение.

Таким образом, видим, что методики конкурентной разведки широко используются специалистами по анализу защищенности, в силу чего, данное направление и стали, возможно ошибочно, относить к информационной безопасности.

Относительно управления репутацией компании – в обычном (штатном) режиме этими вопросами занимаются специалисты по связям с общественностью (Public Relations), но что делать, если, например, в средствах массовой информации оказалась конфиденциальная информация компании или компания подверглась информационной атаке (выброс большого объема негативной информации в СМИ)? На практике, решение этой задачи ложится на плечи специалистов по безопасности компании и, прежде всего, специалистов по информационной безопасности.

Вышеприведенное деление по мерам и должностям, конечно же носит условный характер. Занимая любую из должностей, специалист по защите информации обеспечивает реализацию комплекса правовых, организационных, технических и морально-этических мер.

С точки зрения места информационной безопасности в организационно-штатной структуре компании существует дилемма – относить подразделение информационной безопасности к сфере информационных технологий или к сфере безопасности. В сложившейся практике, в большинстве случаев, подразделение информационной безопасности (служба, отдел, группа и т.п.) входит в структуру подразделения информационных технологий (департамент, управление и т.п.), в редких случаях – в структуру служб безопасности. По мнению автора, это не совсем правильно. Несмотря на то, что в деятельности специалиста по информационной безопасности есть значительный пласт работы, связанный с информационными технологиями, правильнее относить указанное направление деятельности к сфере безопасности и включать в штатную структуру служб безопасности, т.к.:

– как уже рассматривалось в разделе 1, информационная безопасность является частью корпоративной безопасности;

– подчинение специалистов по информационной безопасности руководству служб безопасности минимизирует риск перехода информационных ресурсов под полный контроль подразделения информационных технологий.

Глава 3. Карьера в информационной безопасности

3.1. Что такое карьера?

Карьера – результат осознанной позиции и поведения человека в трудовой деятельности, связанный с должностным и (или) профессиональным ростом.

Должностной рост – изменение должностного статуса человека, его социальной роли, степени и пространства должностного авторитета. Например, переход на вышестоящую должность или переход с должности исполнителя на должность руководителя.

Профессиональный рост – рост профессиональных знаний, умений и навыков, признание профессиональным сообществом результатов труда в конкретном виде профессиональной деятельности. Иными словами, человек может не менять своей должности, но стать признанным специалистом в сфере своей деятельности. Например, стать экспертом по информационной безопасности.

В большинстве случаев должностной и профессиональный рост идут «рука об руку», но, в ряде случаев, бывают и исключения. Например, когда человек сознательно выбирает более глубокое погружение в ту или иную тематику (т.н. «экспертиза»), отказываясь от руководящих должностей, предусматривающих большой пласт работы, связанной с управлением процессами и людьми.

Эксперты в сфере управления персоналом выделяют три вида карьеры (они характерны для любой профессиональной сферы): вертикальная, горизонтальная и портфельная (см. рисунок 2).

Рисунок 2. – Виды карьеры

Вертикальная карьера представляет собой поэтапный рост, прежде всего, должностного статуса человека. Обычно от рядового специалиста, до руководителя. В большинстве случаев, но далеко не всегда, при вертикальной карьере происходит также профессиональный рост, иногда требующий повышения квалификации и (или) получения нового образования (более высокой ступени). Вертикальную карьеру в информационной безопасности можно представить в виде следующей карьерной лестницы – рисунок 3.

Рисунок 3. – Вертикальная карьера в информационной безопасности.

Плюсы вертикальной карьеры:

– рост социального статуса;

– рост дохода (заработной платы);

– личностное развитие, нередко сопровождающееся интересом к предметной сфере и расширением спектра контактов

Минусы вертикальной карьеры:

– повышение ответственности, особенно при переходе на руководящие позиции;

– риск «падения с лестницы» (начла карьеры вновь со стартовых позиций) в случае «отмирания» профессии или ликвидации компании, т.к. одним из основных критериев выбора руководителей в сфере корпоративной безопасности является за частую не наличие развитых компетенций, а лояльность руководству или собственникам компании.

Горизонтальная карьера – данный вид карьеры преимущественно ориентирован на профессиональный рост. При горизонтальной карьере, человек меняет либо сферы деятельности (например, переход из экономической безопасности в информационную) или занимает сходные позиции в различный организациях (например, переходит от заказчика к подрядчику) расширяя, тем самым, профессиональный кругозор, круг контактов и свою экспертность.

Плюсы горизонтальной карьеры:

– профессиональный рост – повышение своих компетенций в одной или нескольких сферах;

– в большинстве случаев не повышается ответственность.

Минус горизонтальной карьеры – отсутствует должностной рост.

Портфельная карьера – суть данного вида карьеры заключается в формировании так называемого «портфеля работодателей» (по аналогии с инвестиционным портфелем). Иными словами, при выборе данного вида карьеры, человек трудоустраивается не к одному, а к нескольким работодателям.

Рисунок 4. – Портфель работодателей

При этом, в соответствии с трудовым законодательством допускается иметь одно основное место работы (оно, как правило, но не всегда, имеет наибольшую долю в портфеле) и любое количество рабочих мест по совместительству.

В качестве примера можно привести портфель работодателей автора (рисунок 4).

Плюсы портфельной карьеры:

– в случае каких-либо карьерных сложностей человек не остается без работы и источника дохода (теряет лишь его часть);

– при работе в разных направлениях, пусть даже и одной профессии, значительно расширяется кругозор и круг контактов.

Минусы портфельной карьеры:

– в сфере информационной безопасности, данный вид карьеры доступен лишь специалистам с экспертной квалификацией, широко востребованным на рынке труда;

– значительное приложение усилий со стороны работника: как правило рабочий день при портфельной карьере превышает стандартный восьми часовой, а значит требуется хорошее умение управлять своим временем и гибкость для того, чтобы планировать свою трудовую деятельность и балансировать между работодателями.

С точки зрения возможностей построения карьеры в сфере информационной безопасности также важно обозначить следующие два направления: работа «у заказчика» и работа «у подрядчика»[4]. Давайте остановимся на них более подробно.

Кто такие «заказчики»? «Заказчики» – это компании, работающие в различных секторах экономики, для которых актуальны вопросы защиты информации и которые реализуют мероприятия по обеспечению информационной безопасности «внутри себя», иногда прибегая к услугам внешних организаций: «аутсорсингу»[5] или «аутстаффингу»[6]. Например, банки, промышленные предприятия, учебные заведения, государственные органы и т. п.

[4] Следует оговориться, что употребление указанных терминов в данном контексте несколько отличается от их значений в действующем гражданском законодательстве.

[5] Аутсо́рсинг – передача организацией, на основании договора, определённых видов или функций своей деятельности другой компании.

[6] Аутстаффинг – использование сотрудников, которые находятся вне штата («аренда сотрудников»).

Кто такие «подрядчики»? «Подрядчики» – это организации, которые оказывают услуги (выполняют работы) по информационной безопасности для сторонних компаний (заказчиков), т.е., по сути, проводят мероприятия по обеспечению информационной безопасности не «внутри себя», а во вне.

В сфере информационной безопасности они, как правило, носят название «системные интеграторы».

Плюсами работы в системном интеграторе, как правило, являются:

– гибкий график работы;

– не требуется значительный опыт (системные интеграторы – это те компании, которые готовы брать на работу перспективных выпускников или студентов);

– веселая атмосфера и насыщенная «корпоративная жизнь».

Минусы:

– низкий уровень оплаты труды (как правило ниже, чем у заказчика);

– не нормированный рабочий день (при большом количестве реализуемых одновременно проектов, рабочий день может значительно превышать стандартные 8 часов).

3.2. Кого сегодня готовят учебные заведения?

Специалистов 1 уровня (см. рисунок 3) – «техников» – готовят в учреждениях среднего профессионального образования.

При этом, следует отметить, что несмотря на соответствие выпускников профессиональным стандартам, спрос на рынке труда на указанных специалистов значительно ниже, чем на специалистов с высшим образованием.

По мнению автора, это связано со следующими причинами:

– отсутствие понимания у большинства работодателей потенциала специалистов со средним профессиональным образованием;

– помимо «психологических» проблем, имеются и законодательные барьеры снижающие преимущества выпускников учреждений среднего профессионального образования по сравнению с высшим профессиональным образованием.

Так, в соответствии с подпунктом «а» пункта 5 «Положения о лицензировании деятельности по технической защите конфиденциальной информации» (утв. постановлением Правительства Российской Федерации от 3 февраля 2012 г. №79), для получения лицензии Федеральной службы по техническому и экспортному контролю России по технической защите конфиденциальной информации, соискатель лицензии должен иметь в штате специалистов имеющих высшее профессиональное образование в области технической защиты информации, либо высшее техническое или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации. Аналогичные требования предъявляются и к соискателям лицензий Федеральной службы безопасности России, осуществляющим деятельность по криптографической защите информации.

Конец ознакомительного фрагмента.