ISSN 2304-120X
КОНЦЕПТ
научно-методический электронный журнал

*Ломовцева О. К. Обучение персонала в условиях обновления регуляторов в сфере обеспечения безопасности информации // Научно-методический электронный журнал «Концепт». – 2017. – № V10. – 0,4 п. л. – URL: http://e-koncept.ru/2017/171039.htm.*

**ART 171039** **УДК 378.046.4:004.9**

***Ломовцева Ольга Константиновна,***
*студентка ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», г. Санкт-Петербург*
o.lomovtceva@gmail.com

# Обучение персонала в условиях обновления регуляторов в сфере обеспечения безопасности информации

***Аннотация.*** *В статье рассматриваются основные требования к обучению персонала в сфере информационной безопасности. Автор показывает важность и необходимость данного процесса; приводит правила его организации, которые регламентируются федеральными регуляторами.*
***Ключевые слова:*** *обучение персонала, информационная безопасность, деятельность регуляторов.*
***Раздел:*** *(01) отдельные вопросы сферы образования.*

В современном мире вопросам защиты информации уделяется большое внимание в силу того факта, что владение информационными ресурсами, недоступными для сторонних компаний на общем с организацией рынке услуг или товаров, может определять самое главное для коммерческих организаций – получение дохода, а для государственных организаций – вопрос защиты интересов государства.

В отношении государственных организаций вопрос защиты информации регулируется со стороны федеральных регуляторов в данной сфере. Регуляторы аккумулируют знания по защите и выпускают руководящие документы, содержащие требования по защите государственных секретов.

Данные знания недоступны для широкой публики в силу их особенностей. Если такие знания станут общедоступными, то и элементы защиты, описанные в них, уже не будут столь актуальными, так как любой может узнать, от чего и какими мерами будет защищен тот или иной объект.

Однако некоторая информация может быть доступна для общественности без ограничений или с частичным ограничением. Эти данные, накопленные путем многолетнего опыта, будут полезны для любой организации, которая задумывается над созданием собственной системы защиты информации или же собирается внести изменения в уже существующую.

Таким образом, любая коммерческая организация может направить своего сотрудника на обучение методам защиты информации, благо таких курсов в наше время имеется огромное множество, а учебные центры, обладающие необходимыми лицензиями, очень часто встречаются в региональных центрах, не говоря уже о больших городах нашей страны.

Чем же страшна потеря информации? Утечка информации возможна везде. Ярким примером может служить информационный портал “WeakyLeaks”, на котором размещались материалы спецслужб США. Вряд ли в данных организациях халатно относятся к защите информации, но тот факт, что такие утечки происходят крайне редко, может говорить о том, что нарушители безопасности, однажды попав в систему, скачали максимум данных за один заход, а не бывают на этих серверах раз в неделю в поисках новинок. Это говорит о том, что утечки бывают, но построенная должным образом система защиты позволяет

свести их к минимуму, а те риски, которых невозможно избежать совсем, можно застраховать или урегулировать при помощи юридических правок.

Конечно, есть замечания, например отсутствие регулирования оповещения о произошедших утечках персональных данных, но утечки информации из информационных систем, обрабатывающих персональные данные, маловероятны при должном выполнении всех требований по защите персональных данных.

В целом в нашем государстве реализована достаточно продуманная законодательная база по защите информации. Существует ряд методических документов, описывающих требования и рекомендации по защите информации ограниченного доступа, (не) содержащей сведений, составляющих государственную тайну Российской Федерации. Многие документы были изданы уже достаточно давно, однако работа над их актуализацией не прекращается.

Информация уже успела стать одним из самых ценных ресурсов в современном обществе. Знание того, что для остальных является секретом, позволяет сделать успешную карьеру или же добиться значительных результатов в том или ином деле. В свете этого желание защитить ключевую для компании информацию становится логичным, а иногда – жизненно важным для организации.

Нарушение конфиденциальности информации может быть связано как с мошеннической деятельностью сотрудников компании, так и с действиями вредоносного программного обеспечения или внешних злоумышленников. Независимо от этого задача защиты конфиденциальных данных должна решаться комплексно: от разработки документации, процедур реагирования и оценки рисков до внедрения технических средств защиты.

Чтобы правильно выстроить систему обеспечения информационной безопасности на предприятии, необходимо не бежать искать продукт А, Б или В, а сначала составить список исходных данных: решаемые задачи (включая защищаемые процессы, поддерживаемые протоколы и системы, производительность и т. п.), отражаемые угрозы, требования нормативных актов, то есть отталкиваться от сценариев использования. И только поняв это, можно переходить к процессу выбора соответствующего решения (и вновь – не продукта, а именно решения).

Специалист по информационной безопасности обеспечивает конфиденциальность данных, предотвращает утечку или несанкционированный доступ к информации, принимает непосредственное участие в создании системы защиты информации, ее аудите и мониторинге, анализирует информационные риски, разрабатывает и внедряет мероприятия по их предотвращению. В его компетенцию также входит установка, настройка и сопровождение технических средств защиты информации [1].

Современные специалисты должны владеть средствами, которые помогут им провести мониторинг безопасности IT-среды, организовать защиту против известных и вновь возникающих угроз, оперативно выявлять и сдерживать любые атаки, а также проводить восстановительные мероприятия. При этом они должны обеспечить свободный и безопасный доступ к корпоративной информации и ресурсам, организовав виртуальные частные сети, построив несколько уровней защиты, обеспечив отказоустойчивость[1], мониторинг и контроль.

В настоящее время обучению персонала уделяется все больше внимания. Компании формируют специальные структурные отделы, которые координируют именно эту часть работы с персоналом, открывается все больше возможностей для обучения – растет количество поставщиков услуг обучения, увеличивается число предлагаемых курсов.

[1] Свойство технической системы сохранять свою работоспособность после отказа одного или нескольких составных компонентов.

Связано это не только с ростом возможностей, но и с переориентированием политики компаний относительно персонала. Сегодня многие стремятся не получить тех, кто знает всё и сразу, а взять молодого сотрудника и обучить «под себя». Конечно, в такой политике больше риска, но и пользы может быть больше.

Специалист по защите информации достаточно востребованная профессия, несмотря на явный кризис на рынке труда. По статистике одного из HR-агентств, специалистам по информационной безопасности в конце 2015 г. предлагали зарплату в среднем на 21% больше, чем в январе 2015 г. Это указывает на то, что даже в условиях кризиса квалифицированные специалисты востребованы; более того, рынок ощущает их нехватку.

Действительно, тема информационной безопасности стала как никогда актуальной – это и набирающие обороты (по уровню ущерба и частоте) атаки банковского сектора (SWIFT, корреспондентские счета), и увеличивающееся количество таргетированных атак (Advanced Persistent Threat, APT) и т. д.

Даже те компании, штат которых укомплектован специалистами по информационной безопасности, нуждаются в квалифицированной оценке зрелости защитных систем, безопасности периметра, веб-приложений и иных элементов инфраструктуры – показательно всё увеличивающееся количество инициаторов BugBounty программ, причем сумма выплат колеблется от $100 до $20000 за уязвимость [2].

Защита информации для участников рынка становится одной из приоритетных задач. Обеспечить такую защиту только автоматизированными средствами практически невозможно. Востребованность специалистов в сфере информационной безопасности (далее – ИБ) растет с той же скоростью, с которой развиваются и сами информационные технологии.

Проблема образования и дальнейшего трудоустройства заключается в извечной проблеме: «Нет работы, потому что нет опыта, потому что нет работы…», и читать эту фразу можно по кругу бесконечно. Общепризнанный факт, что диплом сам по себе не дает приоритета. К моменту выпуска большая часть знаний уже не актуальна.

Сфера защиты информации не исключение, и процессы обучения и повышения квалификации также необходимы в этой области.

В связи с тем что список подконтрольных точек достаточно велик и технологии и знания не стоят на месте, а так или иначе меняются, потребность в изучении нового стоит более чем остро. Однако просто отправить специалиста куда-то на курсы будет недостаточно.

В настоящее время не только коммерческие компании определяют информацию, которую нужно защищать, есть информация, требования к защите которой предъявляются на государственном уровне.

Функции написания рекомендаций, требований и проверки выполнения данных требований выполняют регуляторы. В области защиты информации в России это три основных регулятора: «Федеральная служба по техническому и экспортному контролю» (ФСТЭК), «Федеральная служба безопасности» (ФСБ) и «Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций» (Роскомнадзор) [2].

Как было сказано ранее, одним из основных направлений деятельности регуляторов является формулирование требований по защите информации[2], в частности, это может быть и обновление уже выпущенных ранее норм, и создание совершенно новых – главная мысль в том, что нормы и стандарты с течением времени обновляются и то,

[2] В данной статье рассматриваются только те регуляторы, которые осуществляют свою деятельность в области защиты информации.

что было актуально раньше, может быть упразднено в следующем стандарте. А это, как следствие, влияет не просто на эффективность работы компании и специалистов, а на возможность выполнения тех или иных работ в принципе. Если же разговор идет о государственных заказах или тендерах, объявленных на государственном уровне, недостаток лицензий или прав на проведение тех или иных работ может сильно сказаться как на репутации компании, так и на ее финансовом положении.

Для того чтобы быть в курсе актуальных требований, предъявляемых к защите информации, необходимо отслеживать изменения стандартов и периодически проходить обучение в сертифицированных учебных центрах.

Компании, обладающие (обрабатывающие или просто имеющие доступ) информацией, требования по защите которой определяются государством, невыполнение данных требований ведет к серьезным материальным взысканиям, а иногда и к уголовной ответственности топ-менеджеров организации. Не удивительно, что в данных условиях на обучении персонала пытаются не экономить, благо в современных реалиях существует достаточное количество учебных центров, обеспечивающих возможность всех желающих повысить свою профессиональную грамотность в вопросах безопасности и информации, а также изучить актуальные на данный момент стандарты. Эти знания будет полезны не только тем, кто защищает информацию, регулируемую государством, но и тем, кто занимается обеспечением защиты информации, определенной в коммерческих организациях.

В России самые популярные центры – это:

– УЦ «Информзащита» (http://itsecurity.ru/);
– «Северо-Западный центр комплексной защиты информации» (учебный центр «СЗЦКЗИ») (http://www.szckzi.ru/);
– УЦ «Эшелон» (https://uc-echelon.ru/).

Все центры имеют необходимую аккредитацию в профильных структурах, что позволяет им проводить обучение специалистов по информационной безопасности и выдавать необходимые сертификаты, а также проводить аттестацию специалистов.

Как уже говорилось, обучение сейчас есть во всех сферах. И вместе с развитием компании информация, которую она оберегает, может «обрастать» новыми требованиями либо массивы такой информации могут значительно увеличиваться вместе с компанией. Это могут быть совершенно новые технологии или усовершенствованные старые, новое программное обеспечение или специальные приборы и т. д.

Для эффективной работы в данной сфере мало получить образование и наработать опыт, необходимо свои знания «обновлять», чтобы быть востребованным – для специалиста – и чтобы держаться на рынке – для компании [4].

Как показывает практика, то, что преподается в современных вузах, очень сильно отстает от современного развития технологий безопасности. Об этом говорит и то, что, например, многие учебные пособия, выпущенные в последнее время под редакцией преподавателей российских вузов и рекомендованные для изучения соответствующих специальностей, описывают технологии и продукты 5–7-летней давности. О современных тенденциях в данных материалах говорится мало. Но даже в достаточно актуальных темах слишком много внимания уделяется теории и тем вопросам, которые на практике не применяются, например криптографии. В России принят только один алгоритм шифрования, описанный в ГОСТ 28147-89, – использование любых других алгоритмов является нелегитимным.

Кроме этого даже знание ГОСТ на практике не нужно, так как любой специалист, работающий в государственных или коммерческих структурах, сам никаких криптографических систем не разрабатывает, он работает с тем, что предлагает ему рынок сертифицированных средств шифрования.

В итоге будущему «специалисту» дают знания, которые расширяют его кругозор, но зачастую не нужны в абсолютном большинстве практических ситуаций, за исключением случаев, когда выпускник работает в соответствующих ведомствах или компании-разработчике [5].

В настоящее время, как правило, обучение специалистов инициируется для выполнения той или иной работы. Реже – в соответствии с планом обучения (тренинг-план чаще разрабатывается на крупных предприятиях). Такие меры позволяют не «тратить» бюджет организации на мероприятия, не несущие выгоду, а получать готовых специалистов, так сказать, «под ключ», в нашем случае – под проект.

Помимо обязательных требований к знаниям специалистов, выдвигаемых регуляторами, обучение персонала может быть необходимо для участия в тендере на выполнение заказа.

При анализе возможностей своего персонала и при выявлении недостаточного владения необходимой информацией руководство компании инициирует обучение сотрудника у определенных провайдеров – в учебных центрах (наиболее популярные на территории РФ уже упоминались в данной статье).

Работу провайдеров, в свою очередь, регулируют, то есть выдают лицензии и разрешения на ведение такого рода деятельности, государственные органы: ФСТЭК, ФСБ и Роскомнадзор.

Нормативно-правовые акты, а также международные и отраслевые стандарты предъявляют требования к обеспечению информационной безопасности: обязуют компании принимать меры по охране конфиденциальности информации, также содержат рекомендации по применению организационных мер и технических средств, направленных на защиту конфиденциальной информации (информации ограниченного доступа).

Понятие «конфиденциальность информации» трактуется по-разному, но всегда подразумевает необходимость предотвращения утечки (разглашения) информации.

Таким образом, можно сделать вывод, что обучение специалистов сферы защиты информации носит порой обязательный характер и выдвигает определенные требования не только к самим специалистам, но и к провайдерам обучения, т. е. к учебным центрам. Незнание определенных постановлений в работе с защищаемой информацией может повлиять на успешную дальнейшую деятельность компании и функционирование компании в целом. Из этого следует, что обучение необходимо согласовывать не только с требованиями компании (или бизнеса), но и с регулирующими органами, отвечающими за сохранность государственно важной информации или коммерческой тайны компании.

## Ссылки на источники

1. Официальный сайт учебного центра «Специалист» при МГТУ им. Н. Э. Баумана. – URL: http://www.specialist.ru/
2. Навыки и требования к специалистам по информационной безопасности. – URL: https://habrahabr.ru/company/pentestit/blog/306336/
3. Официальный сайт учебного центра «Информзащита». – URL: http://itsecurity.ru/
4. Официальный сайт ФСТЭК России. – URL: http://fstec.ru/
5. Почему вуз не способен подготовить специалиста по безопасности? – URL: http://www.securitylab.ru/opinion/272388.php?el_id=272388&%3Bclean_reviews_cache=Y&%3BIBLOCK_ID=3&MUL_MODE=&VOTE_ID=102&view_result=Y.

ISSN 2304-120X
КОНЦЕПТ
научно-методический электронный журнал

*Ломовцева О. К. Обучение персонала в условиях обновления регуляторов в сфере обеспечения безопасности информации // Научно-методический электронный журнал «Концепт». – 2017. – № V10. – 0,4 п. л. – URL: http://e-koncept.ru/2017/171039.htm.*

***Olga Lomovtseva,***
*Student of ITMO University, St. Petersburg*
o.lomovtceva@gmail.com

**The importance of personnel training with constantly updated regulators in the field of information security**

**Abstract.** The article contemplates the main requirements to personnel training in the field of information security. The author shows the importance and necessity of this process; lists the rules of its organization which are defined by federal regulators.

**Key words:** personnel training, information security, regulators activities.

**References**

1. *Oficial'nyj sajt uchebnogo centra «Specialist» pri MGTU im. N. Je. Baumana*. Available at: http://www.specialist.ru/ (in Russian).
2. *Navyki i trebovanija k specialistam po informacionnoj bezopasnosti.* Available at: https://habrahabr.ru/company/pentestit/blog/306336/ (in Russian).
3. *Oficial'nyj sajt uchebnogo centra "Informzashhita".* Available at: http://itsecurity.ru/ (in Russian).
4. *Oficial'nyj sajt FSTJeK Rossii.* Available at: http://fstec.ru/ (in Russian).
5. *Pochemu vuz ne sposoben podgotovit' specialista po bezopasnosti?* Available at: http://www.securitylab.ru/opinion/272388.php?el_id=272388&%3Bclean_reviews_cache=Y&%3BIBLOCK_ID=3&MUL_MODE=&VOTE_ID=102&view_result=Y (in Russian).

***Рекомендовано к публикации:***
*Утёмовым В. В., кандидатом педагогических наук;*
*Горевым П. М., кандидатом педагогических наук,*
*главным редактором журнала «Концепт»*

ISSN 2304-120X

**www.e-koncept.ru**

| | | | |
|---|---|---|---|
| Поступила в редакцию *Received* | 10.10.17 | Получена положительная рецензия *Received a positive review* | 25.10.17 |
| Принята к публикации *Accepted for publication* | 25.10.17 | Опубликована *Published* | 31.10.17 |