ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

"Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года" (утв. Президентом РФ 24.07.2013 N Пр-1753)

Настоящими Основами определяются основные угрозы в области международной информационной безопасности, цель, задачи и приоритетные направления государственной политики Российской Федерации в области международной информационной безопасности (далее - государственная политика Российской Федерации), а также механизмы их реализации.

Нормативную правовую базу настоящих Основ составляют Конституция Российской Федерации, международные договоры Российской Федерации в области международной информационной безопасности, федеральные законы, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, иные нормативные правовые акты Российской Федерации.

Настоящие Основы конкретизируют отдельные положения Стратегии национальной безопасности Российской Федерации до 2020 года, Доктрины информационной безопасности Российской Федерации, Концепции внешней политики Российской Федерации и других документов стратегического планирования Российской Федерации.

Настоящие Основы предназначены:

а) для продвижения на международной арене российских инициатив в области формирования системы международной информационной безопасности, включая совершенствование правового, организационного и иных видов ее обеспечения;

б) для формирования межгосударственных целевых программ в области международной информационной безопасности, в осуществлении которых участвует Российская Федерация, а также государственных и федеральных целевых программ в данной области;

в) для организации межведомственного взаимодействия при реализации государственной политики Российской Федерации в области международной информационной безопасности;

г) для достижения и поддержания технологического паритета с ведущими мировыми державами за счет более широкого использования информационных и коммуникационных технологий в реальном секторе экономики.

Под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором

исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

Под системой международной информационной безопасности понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства.

Система международной информационной безопасности призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве.

Сотрудничество в области формирования системы международной информационной безопасности отвечает национальным интересам Российской Федерации и способствует укреплению ее национальной безопасности.

Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"

В настоящей Доктрине используются следующие основные понятия:

а) национальные интересы Российской Федерации в информационной сфере (далее - национальные интересы в информационной сфере) - объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

б) угроза информационной безопасности Российской Федерации (далее - информационная угроза) - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

в) информационная безопасность Российской Федерации (далее - информационная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

г) обеспечение информационной безопасности - осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по

прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

д) силы обеспечения информационной безопасности - государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

е) средства обеспечения информационной безопасности - правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

ж) система обеспечения информационной безопасности - совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

з) информационная инфраструктура Российской Федерации (далее - информационная инфраструктура) - совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

"Паспорт национального проекта "Национальная программа "Цифровая экономика Российской Федерации" (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N

Обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства

"Паспорт федерального проекта "Информационная безопасность" (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 N 9)

Введение. В силу стремительного развития вычислительной техники и программного обеспечения актуальным становится вопрос информационной безопасности и конфиденциальности информации. Потерю информации и получение к ней доступа нелегитимным способом обычно называют атакой (попыткой атаки), или взломом, или хакингом информационной системы, информационной среды. Методы совершения подобных противоправных

действий широко описаны в современной литературе и в настоящем рассмотрении не являются самоцелью. Текущая работа посвящена как раз противоположному процессу - процессу формирования навыков, компетенций информационной безопасности у сотрудников, в чьих должностных обязанностях указано взаимодействие с вычислительной техникой и информационными системами и средами. В настоящее время такое требование относится практически к большинству сотрудников предприятий, организаций, учреждений и т.д. Задача развития знаний и умений у сотрудников весьма обширна. Одной из особенностей является непрерывное обучение информационной безопасности, обусловленное стремительным увеличением программного обеспечения, и уровнем проникновения информатизации в производственные процессы, и совершенствованием способов незаконного доступа к конфиденциальной информации и информационной системе в целом.

Роль человека в процессе обеспечения информационной безопасности. Некоторое время назад считалось, что угроза конфиденциальности, или киберугроза, - явление, характерное для определенного вида деятельности, например платежных систем и банков, и простым пользователям ничего не грозит по причине отсутствия криминального интереса к ним со стороны злоумышленников. При этом производители программных и аппаратных средств уверяли о надежности средств защиты и противодействия угрозам. ИБ возлагалась в большей степени на программное обеспечение. Исходя из числа атак и киберугроз за последние несколько лет говорить о том, что можно избежать кибернападения, недопустимо. Можно говорить о том, как будет организована система управления информационной безопасностью и сколько времени и средств потребуется на устранение последствий кибератаки. По своей методологии все системы программно-аппаратных средств противодействия кибератакам всегда отстают от методов злоумышленников и строят свои системы по противодействию уже известным и совершенным нападениям. При этом стоит отметить важную компоненту ИБ, отличную от программно-аппаратных средств, - это человеческий фактор. Роль человека, пользователя в обеспечении ИБ в настоящий момент остается недооцененной.

Непрерывное обучение информационной безопасности. Только качественная подготовка сотрудников предприятий и специалистов ИБ способна сформировать знания и навыки обращения с конфиденциальной информацией, информационными системами и вычислительной техникой, позволяющие на каждом технологическом этапе их использования соблюдать законы, правила, регламенты и инструкции обеспечения информационной безопасности. Сотрудники, осведомленные о правилах организации и обработки сведений ограниченного доступа и конфиденциальных сведений,

обеспечивают информационную безопасность на долгосрочную перспективу. Ни для кого не секрет, что порядки и регламенты обращения с информацией в электронном виде экстраполированы с соответствующих норм по работе с документами и сведениями на бумажном носителе и лишь учитывают особенность создания, хранения, передачи и обработки электронных документов и информационных систем в целом. Тогда целесообразно признать первостепенную значимость обучения основам безопасности перед традиционными средствами программно-аппаратного обеспечения информационной безопасности на предприятии и в учреждении. При всей необходимости информационных средств противодействия киберугрозам самостоятельно они не могут обеспечить весь комплекс мер информационной безопасности и лишь представляют собой инструмент, хоть и необходимый, но эффективность применения которого определяется тактикой его использования и, как следствие, информационной грамотностью сотрудников подразделений по ИБ. При самом оптимистичном прогнозе согласно резервированной и взаимодополняемой системе управления информационной безопасностью (СУИБ) неизбежно возникает вопрос о сотрудниках, непосредственных пользователях вычислительных средств, которые будут контактировать с системой в процессе выполнения своих должностных обязанностей, об их знаниях и осведомленности об информационной безопасности и конфиденциальности. Отсутствие образования по вопросам безопасности персонала может свести на нет все старания разработчиков и производителей программного обеспечения. Предотвращение возникновения рисков связано в первую очередь с организацией комплексного подхода к обучению и тренировкам персонала в вопросах информационной безопасности. Можно рассматривать различные педагогические методики обучения как с отрывом, так и без отрыва от производства. Разрабатывать систему инструктажа по обеспечению информационной безопасности на одном уровне значимости с аналогичными инструктажами по технике безопасности и доступу к сведениям, составляющим государственную тайну. Информационные технологии могут значительно расширить методики обучения и контроля полученных знаний.

Таким образом, организация регулярного обучения и поддержания его на современном и актуальном уровне обеспечивает упреждающую защиту информации от посягательств, так как каждая ошибка в обращении с информационной системой может быть использована злоумышленниками. Можно привести самурайское выражение: "Враг стоит, и я неподвижен, враг напал, но я ударил первым". Упреждающим ударом в информационной безопасности и является система своевременного и актуального обучения обеспечению информационной безопасности на предприятии.

Традиционно меры по обеспечению информационной безопасности включают пять пунктов: законодательный (законы, нормативные акты, стандарты и т.п.), морально-этический (всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации), административный (действия общего характера, предпринимаемые руководством организации), физический (механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей), аппаратно-программный (электронные устройства и специальные программы защиты информации).

Необходимым и одним из основных компонентов, на наш взгляд, является обучение сотрудников основам информационной безопасности, развитие у них навыков и умений и, как следствие, формирование культуры информационной безопасности. В доктринах информационной безопасности стран НАТО 2017 и 2018 гг. первоочередной задачей, проходящей красной нитью, является всестороннее обучение персонала, сотрудников и рядовых граждан основам обеспечения информационной безопасности. Непрерывное повышение квалификации сотрудников, прохождение ими стажировок и т.д.

Формирование культуры информационной безопасности является многогранным педагогическим процессом, заслуживающим всестороннего исследования и изучения.

Трудности в реализации повышения квалификации по информационной безопасности. Надежность любой программы информационной безопасности определяется прочностью ее самого слабого звена. Достаточно часто самым слабым элементом в программе управления информационной безопасностью являются люди. Люди неосознанно нажимают на вложения электронной почты, выбирают небезопасные пароли и в некоторых случаях делятся этими паролями с коллегами, становятся жертвами умных - и не очень умных - атак социальной инженерии, или они просто обходят установленные средства информационной безопасности с целью повышения производительности выполняемых производственных задач.

Большинство коммерческих и частных организаций воспринимают задачу обучения персонала и повышения квалификации в области безопасности достаточно сложной и не обладающей наглядной краткосрочной эффективностью. Такому подходу потворствует желание экономии финансовых и людских средств, а также перегрузка и нежелание сотрудников воспринимать слишком большое количество информации. На март 2019 г., по данным департамента по цифровым технологиям, культуре, СМИ и спорту Великобритании, отмечаются базовые технические пробелы по кибербезопасности у 54% коммерческих организаций и 18% государственных

организаций в Великобритании. Кибербезопасность - достаточно сложное понятие, не определяющееся только количеством квалифицированного технического персонала, это определенный уровень грамотности и навыков всего персонала в сочетании с техническими подходами, идущими в ногу со временем.

В бюджетных и государственных организациях ситуация обстоит лучше из-за строгой законодательной регуляции деятельности. Развитие законодательной базы - важный и необходимый элемент, направленный на обеспечение ИБ, имеющий одну особенность, связанную с необходимостью постоянных изменений для противодействия современным киберугрозам. Изменения в законодательстве и нормативных актах приводят к выполнению конкретных требований, указанных в документах, без комплексного анализа безопасности. Такому же пути следуют и при обучении персонала, проводимом исключительно для соответствия нормативным требованиям и регламентам. В результате информационная безопасность рассматривается как препятствие для способности бизнеса предоставлять эффективные услуги клиентам и развития, а впоследствии вообще игнорируется.

Рассмотрим один из характерных сценариев попытки управления информационной безопасностью предприятия. Допустим, на организацию распространялись многие отраслевые нормы, а также юридические обязательства согласно действующему законодательству, например Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" или Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". Различные инициативы по повышению грамотности сотрудников в вопросах информационной безопасности потерпели неудачу, и недавно назначенному главному сотруднику по информационной безопасности было поручено разработать программу по повышению квалификации персонала по информационной безопасности, которая бы учитывала все потребности.

В результате обзора различных внутренних программ был выявлен ряд инициатив по повышению осведомленности о безопасности, которые были начаты в соответствии с действующими регламентами и указаниями. Тем не менее результаты обзора показали, что каждая из этих инициатив по повышению уровня информационной грамотности была сосредоточена исключительно на своем собственном индивидуальном направлении и не была связана с общей задачей информационной безопасности предприятия в целом. Это, в свою очередь, привело к дублированию усилий, что послужило тому, что персонал и даже руководство стали рассматривать обучение основам информационной безопасности как пустую трату времени.

Другим ключевым элементом, который был определен как причина провала этих программ, было отсутствие поддержки со стороны высшего руководства для различных программ по повышению безопасности. Каждая из программ была поддержана непосредственным руководителем, ответственным за конкретное направление бизнеса и реализацию информационной безопасности в нем. Однако за пределами этого направления поддержка программы была незначительной или отсутствовала, и, хотя намерения были хорошими, во многих случаях программы по обеспечению безопасности не работали из-за того, что руководство других направлений бизнеса не рассматривало программу как проблему с высоким приоритетом. Сотрудники службы ИБ такой организации столкнулись с непониманием и скептическим отношением к проблеме внедрения программы обучения информационной безопасности сотрудников.

Система управления информационной безопасностью. Наиболее эффективным способом обеспечения успеха будет создание СУИБ, которая могла бы отвечать всем нормативно-правовым требованиям. Для этой цели можно использовать Стандарт информационной безопасности Международной организации по стандартизации/Международной электротехнической комиссии (ISO/IEC) 27001. Ранее известный как BS 7799, ISO/IEC 27001 в настоящее время является международно признанным стандартом, который предоставляет компаниям основанный на риске подход к защите своей информации. Являясь международным стандартом, ISO/IEC 27001 предоставляет организациям независимую проверку того, что их система управления информационной безопасностью соответствует международно признанному стандарту. Это дает компании, ее клиентам и партнерам уверенность в том, что они управляют своей безопасностью в соответствии с признанными и проверенными рекомендациями и регламентами.

Принимая основанный на рисках и стандартах подход к внедрению системы управления информационной безопасностью в соответствии с ISO/IEC 27001, компании получают преимущества за счет соответствия законодательным и отраслевым нормативным требованиям.

Важно отметить, что ISO/IEC 27001 можно просто использовать в качестве основы, на которой компания может внедрять и оценивать свою систему управления информационной безопасностью без необходимости аккредитации или регистрации. Это особенно полезно для компаний, желающих убедиться, что они внедряют эффективную СУИБ, но, возможно, не хотят затрат и накладных расходов на проведение аудита.

В Стандарте информационной безопасности ISO/IEC 27001 был ряд ключевых элементов. Рассмотрим их подробнее.

Одним из ключевых факторов успеха любой реализации ISO/IEC 27001 является комплексный подход к управлению рисками в системе управления информационной безопасностью предприятия или учреждения. Выявив все риски информационной безопасности, с которыми сталкивается организация, и уровень риска, который руководство и бизнес готовы принять, можно выбрать и внедрить наиболее подходящие средства для управления этими рисками в рамках приемлемых уровней риска.

Обычно выявляется риск несоблюдения различных нормативных и правовых требований. Некоторые из этих нормативных и правовых требований предусматривают, что сотрудники должны быть осведомлены о своих обязательствах в соответствии с этими правилами и должны пройти соответствующее обучение.

Кроме того, стандарт информационной безопасности ISO/IEC 27001 требует, чтобы оценка рисков проводилась регулярно, чтобы можно было измерять эффективность выбранных средств контроля, а также выявлять новые риски и управлять ими. Это гарантирует, что программа осведомленности о безопасности должна впоследствии обновляться при выявлении новых рисков. Это позволяет актуализировать программу и учитывать в ней современное состояние угроз и мер противодействия.

Поскольку отсутствие обучения сотрудников по вопросам соблюдения требований информационной безопасности было выявлено при оценке риска, им необходимо впоследствии управлять и принимать меры по устранению недостатка. Принятие таких мер в рамках бизнеса или предприятия относится к компетенции высшего руководства. Одним из способов управления этим риском является реализация программы обучения по обеспечению информационной безопасности. Принятие такого решения должно было быть признано и одобрено старшим руководством, специалист подразделения информационной безопасности должен получить полную поддержку старших руководителей, чего так не хватало прежде.

После поддержки программы устранения рисков, вызванных нехваткой обучения, формируются необходимые программы, средства и ресурсы.

Непрерывное улучшение. Одним из ключевых преимуществ внедрения системы управления информационной безопасностью на основе стандарта информационной безопасности ISO/IEC 27001 является требование постоянного совершенствования СУИБ.

Возможность разработки обучающей программы по вопросам безопасности и конфиденциальности, которая отвечала бы реальным потребностям бизнеса, также обеспечивает успех обучения сотрудников и информационной безопасности в целом.

Наряду с предоставлением прочной основы для разработки программы обучения по вопросам безопасности и конфиденциальности СУИБ использует стандарт:

- для соблюдения законодательства:

наличие структурированной системы управления информационной безопасностью облегчает задачу определения требований соответствия законодательству. Это также сделало включение новых или изменение прежних требований соответствия программ обучения осведомленности и информационной безопасности и конфиденциальности более эффективным и действенным процессом;

- улучшенного управления:

наличие единой программы обучения по вопросам безопасности и конфиденциальности также обеспечивает уверенность руководства в соблюдении ключевых элементов информационной безопасности, изучению которых и посвящено обучение персонала. Старшее руководство также осознает эффективность посещения курсов. Эта информация позволяет руководству обеспечить прозрачную и эффективную кадровую политику, направленную на назначение на ключевые посты сотрудников, обладающих знаниями в области информационной безопасности. Тестовые материалы, разработанные для поддержки учебной программы, также позволили руководству быстро определить, где были пробелы в обучении и какие дополнительные инвестиции необходимо было сделать для устранения этих пробелов;

- улучшения отношений с клиентами и партнерами:

после демонстрации компанией серьезного отношения к информационной безопасности клиенты и торговые партнеры могут уверенно обращаться к ней, зная, что она применила независимый проверяемый подход к управлению рисками информационной безопасности.

Выводы. Благодаря использованию программы обучения по вопросам информационной безопасности и конфиденциальности в соответствии с ISO/IEC 27001, в отличие от прежних не структурированных и не систематизированных отдельных программ, снижается стоимость обучения персонала, и повышается отдача от обучения, и оправдываются вложенные инвестиции в обучение.

Хотя ISO/IEC 27001 не гарантирует 100%-ную безопасность (в принципе никакой стандарт или система не может), он позволяет компании применять качественный подход к защите данных своих клиентов и в конечном итоге к защите конфиденциальности личной информации своих клиентов.