УДК 65.0
DOI: 10.33764/2618-981X-2021-6-235-239

ОБОСНОВАНИЕ НЕОБХОДИМОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В ЭПОХУ ЦИФРОВИЗАЦИИ

Антон Владимирович Обиденко
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры информационной безопасности, e-mail: obidenko@rambler.ru

Аэлита Владимировна Шабурова
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор экономических наук, профессор, зав. кафедрой фотоники и приборостроения, директор института оптики и технологий информационной безопасности, тел. (383)344-40-58, e-mail: aelita_shaburova@mail.ru

Актуальность исследования состоит в обеспечении информационной безопасности, оптимизацию затрат на защиту данных, а также уменьшение информационных рисков организации. Результаты исследования позволят усовершенствовать и повысить качество защиты данных при помощи методов, алгоритмов и процедур при создании концепции информационной безопасности организации, основной целью которой является снижение рисков.

Ключевые слова: информационная безопасность, безопасность предприятия, риски

JUSTIFICATION OF THE NEED TO ENSURE INFORMATION SECURITY OF AN ENTERPRISE IN THE ERA OF DIGITALIZATION

Anton V. Obidenko
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Information Security, e-mail: obidenko@rambler.ru

Aelita V. Shaburova
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Professor, Head of Department of Photonics and Device Engineering, Director, Institute of Optics and Information Security Technologies, phone: (383)344-40-58, e-mail: aelita_shaburova@mail.ru

The relevance of information security research aimed at reducing information risks and optimizing enterprise costs for information protection. The results make it possible to increase the degree of information protection at enterprises by using methods, algorithms and practical procedures in the formation of an information security system aimed at reducing information risks.

Keywords: information security, enterprise security, risks

Введение

Актуальность исследования обосновывается обострением ситуации с информационной безопасностью (ИБ) в рамках стремительного развития технологий и инструментов защиты данных. На это указывает значительный рост инци-

дентов информационной безопасности и их неутешительные последствия. Если обратиться к статистике, то при утечке с предприятия уже 20 % информации, составляющих коммерческую тайну, в половине случаев такая организация оказывается банкротом. Девять из 10 предприятий с заблокированной или утраченной информацией на период свыше 10 дней уходят из бизнеса, при этом почти половина из них сразу заявляет о своей недееспособности.

Цифровизация – процесс, требующий основательного внесения изменений в промышленные технологии, финансовые транзакции, принципы создания новых продуктов и услуг. Это не просто набор IT-решений в организациях и на производстве, а масштабная переоценка подходов и стратегий в бизнесе, реализуемая с помощью IT-технологий. Это интеграция, ежедневно используемых, офисных и промышленных технологий с совершенно новыми IT-направлениями, такими как облачные вычисления, искусственный интеллект, машинное обучение, IoT и т.д. Не все организации готовы к совершенно новым требованиям, которые им предъявляет цифровизация, например, к совершенствованию методов ведения бизнеса, изменению внутренних бизнес-процессов и взаимодействия. Руководство должно быть подготовлено, как к положительным, так и к отрицательным ее последствиям, т.к. привнесенные изменения в бизнес цифровизацией создали существенные проблемы для информационной безопасности, возникли новые направления угроз и значительно увеличилось количество уязвимостей для потенциальных киберпреступлений.

Существующие проблемы информационной безопасности в условиях цифровизации:

– непрозрачность событий ИБ в корпоративной инфраструктуре предприятий;

– трудности с вопросом автоматизации всех процессов ИБ;

– интеграция решений ИБ;

– гибкое масштабирование.

Рассмотрим каждую проблему в отдельности.

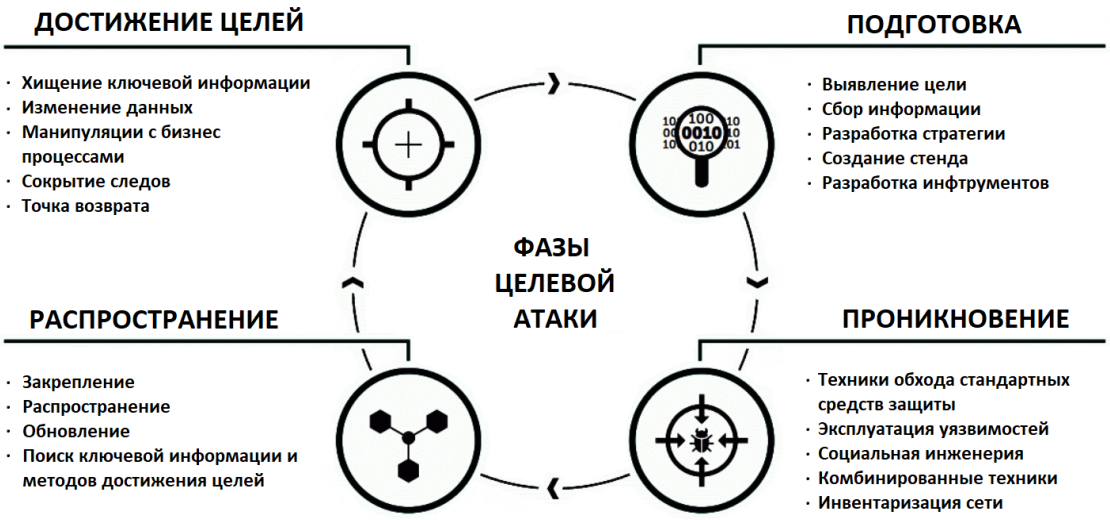
Непрозрачность событий ИБ в корпоративной инфраструктуре предприятий. В больших организациях применяются разнообразные технические локации, основанные на облачный сервисах, при этом оборудованные своими инструментами ИБ, а также различными внутренними сервисами. Но, все еще имеются трудности, равно как с интеграцией подобных решений, так и с фиксацией и прозрачностью событий и инцидентов ИБ в такого рода IT-инфраструктуре. Помимо этого, цифровизация подразумевает существенное увеличение облачных решений и усложнение комплексной организационной инфраструктуры путем использования IoT, блокчейна, ИИ т.д.

Трудности с вопросом автоматизации всех процессов ИБ. Во многих организациях, обычных и крупных, все еще остаются неавтоматизированными большинство процессов информационной безопасности, при всем при этом даже не сформирован план по их автоматизации. Руководители отделов ИБ подобных организаций полностью уверены в том что они защищены со всех сторон, равно как изнутри периметра, так и в облачных сервисах, мобильных устройствах, web-

серверах и т.д. Вероятно, некоторые решения ИБ (сетевые экраны, антивирусное ПО, системы выявления атак и т.д.) могут предоставить определенную степень защиты на некоторых участках, а также снижают число инцидентов ИБ, однако в отсутствии формирования единой стратегии и политики безопасности в такого рода компании в будущем непременно начнутся проблемы с информационной безопасностью.

Интеграция решений ИБ. Нужно заметить, что в основном компании не уделяют должного внимания интеграции многих решений информационной безопасности, отсутствует прозрачность видимости существующих угроз, недостаточный контроль соответствия требованиям, которые предъявляют регуляторы.

Гибкое масштабирование. Согласно статистике, в сфере информационной безопасности специалистами установлено то, что в большом числе компаний, часть организационной инфраструктуры все еще остаётся беззащитной. По мере того, как увеличивается ИТ-инфраструктура, спровоцированная глобальной цифровизацией, а также из-за более ухищренных киберпреступлений, возникает необходимость в масштабируемости решений информационной безопасности. Даже в случае, если в организации существуют эффективно действующие решения, частично защищающие элементы IT-инфраструктуры (к примеру, сетевые экраны, антивирусное ПО и т.д.), степень защищенности организации в целом не увеличивается, ввиду слабой интеграции и масштабируемости данных раздельных решений. Угрозы, связанные с обновлением ПО, вызывают опасения по сей день, т.к. очень часто с ПО, незаметно для пользователя, интегрирована вредоносная составляющая, показанная на рисунке.



Фазы целевой кибератаки

Большие организации гораздо чаще внедряют собственные продукты информационной безопасности в общую архитектуру корпоративной защиты. Необходимо выделить, что в подобных организациях предпочитают подходить стратегически и формируют политику безопасности, что дает возможность:

– своевременно выявлять угрозы и незамедлительно реагировать;

– предоставлять высококачественную защиту информационных активов;

– располагать прозрачной технологической средой с целью выявления угроз.

В результате проведенного анализа можно установить цель исследования, она заключается в разработке методов и средств обеспечения информационной безопасности организации, направленных на снижение ее информационных рисков:

– подготовить план информационной безопасности организации;

– составить список ресурсов, в отношении которых должны соблюдаться свойства конфиденциальности и целостности информации, в противном случае следует серьезный и непоправимый вред организации; определить основные векторы угроз;

– составить концепцию информационных рисков, сформировать методы оценки, а также управляющие инструкции;

– организовать метод оценки остаточных рисков в организации;

– составить схему метода расчета расходов на управление информационной безопасностью, а также вычисление ее финансовой оправданности.

Теоретическая и практическая важность исследования заключается в формировании концепции информационной безопасности в организации, основанной на риск-анализе. Результаты исследования дадут возможность повысить уровень защиты данных в организациях посредством применения некоторых практических процедур при создании концепции информационной безопасности, вследствие чего будет достигнуто сокращение рисков. Актуальность исследования состоит в создании методов реализации информационной безопасности организации, нацеленных на определение угроз нарушения основных свойств защищаемой информации, т.е. целостности и конфиденциальности данных, составление плана, а также вычисление рисков и подтверждение обоснованности вложений в информационную безопасность с экономической точки зрения.

Выводы

На данный момент имеется длинный список угроз информационной безопасности, нарушений, киберпреступлений, требуется научный подход в систематизации, а также дополнительная оценка сопряженных с ними рисков. Необходимо также разработать профилактические мероприятия по части их предупреждения.

Проведенные исследования говорят о том, что отсутствие обдуманной утвержденной политики обеспечения информационной безопасности является главным фактором существующих проблем организаций в сфере защиты данных, основанной на организационных резолюциях с дальнейшим контролем выполнения и эффективной оценкой.

Все это наталкивает на потребность разработки научно аргументированных методов обеспечения информационной безопасности частных организаций, фи-

нансовых учреждений, банков, предусматривающих положительный опыт отечественных, а также иностранных организаций в данной сфере. Совокупность данных вопросов подразумевает проработку актуальных и целесообразных методов с целью их решения. Исходя из вышесказанного можно, обозначить цели и задачи исследования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Норткан С., Купер М., Фирноу М. и др. Анализ типовых нарушений безопасности в сетях [Пер. с англ. под ред. А.А. Чекаткова]. М. : Вильямс, 2001.

2. Байбурин В.Б., Бровкова М.Б., Пластун И.Л. и др. Введение в защиту информации : учеб. пособие. М. : ФОРУМ-ИНФРА-М, 2004.

3. Баутов А.Н. Программно-методическое обеспечение «Расчет рисков и вычисление оптимальных затрат на систему защиты информации от несанкционированных действий и сохранение конфиденциальности информационных ресурсов». М., 2001.

4. Баяндин Н.И. Технологии безопасности бизнеса. М. : Юристъ, 2002.

5. Гаценко О.Ю. Защита информации. Основы организационного управления. СПб. : изд. дом «Сентябрь», 2001.

6. Голиусов А.А., Дубровин А.С., Лавлинский В.А. и др. Методические основы проектирования программных систем защиты информации. Воронеж: ВИРЭ, 2002.

7. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. С-Пб. : БХВ-Петербург, 2003.

8. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах: Программ.-аппарат. средства обеспечения информ. безопасности : учеб. пособие. М. : Радио и связь, 2000.

9. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. М. : Гелиос-АРВ, 2002.

10. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия. М. : Дашков и К, 2004.

11. Семкин С.Н., Семкин А.Н. Основы информационной безопасности объектов обработки информации: науч.-практ. пособие. М., 2000.

12. Стрельцов А.А. Обеспечение информационной безопасности России. М.: МЦНМО, 2002.

13. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации: Учебное пособие. М.: Гелиос АРВ, 2005.

14. Ярочкин В.И. Информационная безопасность: учебник для вузов. М., Фонд «Мир», 2003.