УДК 004

Оценка и мониторинг защищенности информационных ресурсов как нештатная ситуация

Комаров В. В.[1], **Буйневич М. В.**[2] ✉

[1]АНО ДПО «Центр повышения квалификации «АИС»
Москва, 111123, Российская Федерация
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Постановка задачи: *контроль (оценка) и мониторинг эффективности системы защиты информации (СЗИ) являются неотъемлемой частью процесса эксплуатации защищаемых объектов информатизации (государственных информационных систем, информационных систем персональных данных, значимых объектов критической информационной инфраструктуры). Несовершенство средств контроля и мониторинга СЗИ вкупе с уязвимостями последней зачастую приводит к возникновению компьютерных инцидентов с последующим нарушением работоспособности и/или деградацией защищаемого объекта информатизации. Одним из эффективных путей решения данной проблемы является организация и проведение профилактических мероприятий.*

Главная ***цель работы*** *– уменьшение времени реагирования и ликвидации последствий от компьютерного инцидента, вызванного проведением мероприятий по контролю (оценке) эффективности СЗИ за счет планирования действий при нештатной ситуации, обучения и тренировки персонала необходимым действиям, материально-технического и прочих видов обеспечения такого рода деятельности.*

Дополнительной ***целью*** *является нейтрализация угроз безопасности информации, реализуемых внешним нарушителем с использованием социотехнических методов (фишинг).*

Методы: *обобщение и анализ существующего нормативно-правового и методического обеспечения действий подразделений информационной безопасности по проведению контрольных (оценочных) мероприятий, а также при нештатных ситуациях и возникновении компьютерных инцидентов.*

Новизна: *элементами новизны представленной работы является рассмотрение мероприятия по контролю (оценке) эффективности СЗИ как нештатной ситуации при эксплуатации защищаемого объекта информатизации.*

Результаты: *доказана необходимость введения нового класса угрозы безопасности информации – угроза нарушения работоспособности информационного ресурса, вызванного проведением мероприятий контроля (оценки) и мониторинга эффективности СЗИ.*

Практическая значимость: *результаты работы могут быть использованы для обеспечения безопасности информационных ресурсов организации при проведении Центром защиты информации и специальной связи Федеральной службы безопасности Российской Федерации и территориальными органами безопасности в отношении их мероприятий по оценке их защищенности и способности органов (организаций) противостоять угрозам информационной безопасности.*

Ключевые слова: *информационные ресурсы, система защиты информации, компьютерный инцидент, внешний нарушитель, мониторинг и оценка защищенности, угроза безопасности информации, нештатная ситуация*

Библиографическая ссылка на статью:
Комаров В. В., Буйневич М. В. Оценка и мониторинг защищенности информационных ресурсов как нештатная ситуация // Информационные технологии и телекоммуникации. 2023. Т. 11. № 4. С. 1–14. DOI: 10.31854/2307-1303-2023-11-4-1-14

Reference for citation:
Komarov V., Buinevich M. Assessment and Monitoring of the Security of Information Resources as an Emergency Situation // Telecom IT. 2023. Vol. 11. Iss. 4. PP. 1–14. (in Russian) DOI: 10.31854/2307-1303-2023-11-4-1-14

Введение

Мониторинг и оценка защищенности информационных ресурсов в организации позволяет выявить слабости в системе защиты информации (СЗИ) и оперативно устранить их, либо, применяя компенсирующие меры безопасности, нейтрализовать потенциальные угрозы безопасности информации [1]. Важность проведения мониторинга и оценки отмечена в действующих общих требованиях Регуляторов по защите различных информационных ресурсов, таких как: информационные системы персональных данных, автоматизированные системы управления технологическим процессом, государственные информационные системы, значимые объекты критической информационно инфраструктуры[1], – а также в документах отраслевой и ведомственной направленности[2] [2].

Мониторинг и оценка проводится как органом (организацией) самостоятельно, так и с привлечением специализированных организаций, имеющих соответствующие лицензии Регулятора на деятельность по защите информации (приказ ФСТЭК России от 21.12.2017 № 235). В интересах государства мониторинг и оценка осуществляется уполномоченными органами власти в рамках контрольно-надзорной деятельности и в рамках системы государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)[3].

---

[1] Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования.

[2] Постановление Правительства РФ от 13.05.2022 № 860 «О проведении эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений» (вместе с «Положением о проведении эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений»).

Указание Банка России от 29.09.2016 № 4144-У.

О требованиях к системе управления рисками, связанными с осуществлением репозитарной деятельности, и правилам управления рисками репозитария.

[3] Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

DOI: 10.31854/2307-1303-2023-11-4-1-14
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/1-14.pdf

В нормативных требованиях по защите информации периодичность и длительность внутренних мероприятий по мониторингу и оценке установлена только по верхней границе – не реже, чем раз в три года. Серьезно ужесточены требования к процедуре оценки в отношении аттестованных информационных ресурсов – не реже, чем раз в два года, более того – протоколы с результатами оценки должны в обязательном порядке направляться в ФСТЭК России (приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»).

Проводятся исследования, направленные на дальнейшее снижение погрешности проводимой оценки и повышение достоверности ее результатов, разрабатываются и внедряются более совершенные методы мониторинга (оценки) [3–11]. Основной интерес в данном исследовании вызывают мероприятия мониторинга и оценки, независимые от органа (организации) – проводимые органами власти в рамках действующего законодательства Российской Федерации.

Необходимо отметить, что в зарубежных странах отсутствует подобный подход в силу иной роли государственных органов в обеспечении информационной безопасности организаций, а результаты соответствующей работы специальных служб иностранных государств относятся к сведениям ограниченного доступа.

Постановка задачи

До 2022 г. органы (организации) сталкивались со следующими видами оценки:

– ФСТЭК России – в рамках мероприятий государственного контроля;

– Национальный координационный центр по компьютерным инцидентам (НКЦКИ) – в рамках функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации (ГосСОПКА).

ФСТЭК России для оценки при проведении государственного контроля используют сертифицированные по требованиям безопасности информации программные и аппаратно-программные средства контроля. Возможность и порядок использования таких средств контроля обязательно согласуется с руководителем органа (организации) с учетом особенностей функционирования значимого объекта критической информационной инфраструктуры (Постановление Правительства РФ от 17.02.2018 № 162).

Методика проведения оценки от НКЦКИ (https://gossopka.ru/upload/iblock/a63/hwj5wwz7is5zm42pyzl587s52jubuer7/Metodicheskie-rekomendatsii-po-otsenke-stepeni-zashchishchennosti.pdf) прямо указывает на необходимость учитывать требования к непрерывности функционирования информационных ресурсов и не применять методы и способы оценки, которые могут привести к нарушению функционирования информационных ресурсов органов (организаций).

После введения в мае 2022 г. дополнительных мер по информационной безопасности, в отношении ограниченного перечня органов (организаций) появились требования о выполнении оценки с техническими требованиями от Минцифры России[4]. Подход последнего к проведению оценки уровня защищенности включал в себя требования об обязательном проведении внешней оценки путем привлечения к ней на договорной основе организации, имеющей соответствующую лицензию ФСТЭК России. При этом, основным условием к исполнителю указывалось заблаговременное согласование с органом (организацией) любых действий, которые могут привести к негативным последствиям или нарушениям функционирования информационной инфраструктуры[5].

Таким образом, возможность и порядок применения специальных средств при оценке подлежат согласованию с органом (организацией) вне зависимости от типа проверки (внутренняя, внешняя или в рамках контрольно-надзорной деятельности). С безусловным приоритетом недопущения наступления негативных последствий при проведении оценки.

В июне 2022 г. был опубликован приказ ФСБ России от 11.05.2023 № 213 «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими», устанавливающий порядок мониторинга защищенности информационных ресурсов (далее – приказ ФСБ № 213). Впервые органы (организации) столкнулись с ситуацией, когда установленный порядок мониторинга, включающий в себя как одну из форм – оценку, не только не согласовывался с ними по возможности и порядку применения специальных программных и программно-аппаратных средств оценки, но и прямо предусматривал наступление негативных последствий для оцениваемых информационных ресурсов. Таким образом, сам уполномоченный орган власти по контрольно-надзорной деятельности ГосСОПКА указал в нормативно-правовом акте на актуальность и опасность проводимых мероприятий для защищаемого информационного ресурса.

---

[4] Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Распоряжение Правительства РФ от 22.06.2022 № 1661-р «Об утверждении перечня ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России».

[5] Типовое техническое задание на выполнение работ по оценке уровня защищенности информационной инфраструктуры. Минцифры России. 03.06.2022. URL: https://digital.gov.ru/ru/documents/8235

DOI: 10.31854/2307-1303-2023-11-4-1-14
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/1-14.pdf

Учитывая вышеизложенное, возникла необходимость рассмотреть мероприятие оценки не только как обязательную меру безопасности при эксплуатации информационного ресурса, но и как ситуацию, в ходе развития которой возникают негативные последствия, вызванные нарушениями функционирования информационных ресурсов. Так как, в силу отсутствия подобных нормативно-правовых документов, при проектировании и создании информационных ресурсов данный подход не применялся, то такую ситуацию следует отнести к нештатным. Сложившаяся ситуация потребовала более детального исследования на предмет выявления возможных критериев, объективно влияющих на возможность возникновения негативных последствий при различных типах оценки и выработки предложений, направленных на минимизацию их масштаба.

Результаты исследования и их обсуждение

Результаты исследования критериев, влияющих на возможность возникновения негативных последствий при проведении оценки, отображены в таблице 1.

Таблица 1 – Сводные сведения по критериям, влияющим на возникновение негативных последствий при проведении оценки различными органами (организациями)

Критерии	Кто проводит мероприятия оценки		
	Владелец / оператор (лицензиат ТЗКИ)	ФСТЭК России	ФСБ России
Используемые методы оценки	согласованы	согласованы	без согласования, не известны
Используемые средства оценки	согласованы	согласованы	без согласования, не известны
Длительность проведения	согласованная	не более 20 рабочих дней	не ограничено
Даты проведения	согласованные	плановые	плановые
Время проведения	согласованное	согласованное	без согласования, не известно
Время на подготовку к проведению оценки	согласованное	14 дней / 1 день*	14 дней
Подключение	внешнее / внутреннее	внутреннее	внешнее / внутреннее
Режим работы СЗИ	обычный / усиленный	обычный / усиленный	обычный / ослабленный
Противодействие внешним подключениям	допускается	не требуется	запрещено
Наступление негативных последствий	не допускается	не допускается	допускается

DOI: 10.31854/2307-1303-2023-11-4-1-14
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/1-14.pdf

Критерии	Кто проводит мероприятия оценки		
	Владелец / оператор (лицензиат ТЗКИ)	ФСТЭК России	ФСБ России
Время прекращения оценки при наступлении негативных последствий	минимально	минимально	более 2 часов
Время на ликвидацию последствий негативных событий	любое	любое	не более 6 часов
Наличие информации об оцениваемом ресурсе	согласованное	полная информация	полная информация
Наличие информации об особенностях функционирования СЗИ (уязвимости, недекларированные возможности)	ограниченное	полная информация**	полная информация**
Ответственность лиц, проводящих оценку, за наступление негативных последствий	уголовная, гражданско-правовая, дисциплинарная	дисциплинарная	дисциплинарная

Примечания:

*При проведении внепланового государственного контроля ФСТЭК России срок уведомления органа (организации) сокращается до одного дня (приказ ФСТЭК России от 29.04.2021 № 77).

**Органы (организации) используют для защиты своих информационных ресурсов СЗИ, прошедшие оценки соответствия в системах сертификации ФСБ России и ФСТЭК России.

Из сведений, представленных в таблице 1, следует, что, во-первых, максимально безопасно проведение оценки, проводимое органом (организацией), за счет выбора ее времени, средств, методов и объемов. Во-вторых, мероприятия ФСТЭК России практически безопасны. Снижение безопасности происходит только из-за отсутствия согласования с органом (организацией) периода оценки, но сохраняется возможность ее проведения в «технологические окна» (согласование времени проведения) и ограничить использование потенциально опасных инструментов оценки. И, в-третьих, мероприятия ФСБ России потенциально максимально опасны, поскольку практически исключается возможность избежать возникновения негативных последствий.

Результаты проведенного анализа позволяют сделать вывод о применимости методического документа ФСТЭК России «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021) при проведении мероприятий оценки в рамках приказа ФСБ № 213, поскольку «налицо» все атрибуты угрозы:

DOI: 10.31854/2307-1303-2023-11-4-1-14
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/1-14.pdf

– источник возникновения угрозы безопасности информации носит антропогенный характер;

– возможно наступление негативных последствий в виде нарушения штатного функционирования информационных ресурсов органа (организации);

– негативные последствия наступают вследствие несанкционированного воздействия на информационный ресурс органа (организации);

– воздействие на информационные ресурсы происходит с использованием подключаемых по сетевым протоколам программно-аппаратных комплексов органов безопасности.

Отсутствие прямого умысла на достижение негативных последствий (намерения) не исключает отнесение мероприятий оценки к антропогенным источникам угроз безопасности информации (нарушителям), так как ФСТЭК России указал на обязательность оценки угроз, носящий непреднамеренный характер (непреднамеренные угрозы) («Методика оценки угроз…»). Таким образом, мы имеем возможность оценить угрозы безопасности информации, возникшие вследствие непреднамеренных, неосторожных или неквалифицированных действий сотрудников, реализуемых в рамках приказа ФСБ № 213.

Модель нарушителя и угроз

Определим вид нарушителя, его потенциал и последствия.

В отличие от вида нарушителя «специальные службы иностранных государств», для которого ФСТЭК России установлен максимальный уровень возможностей – Н4, принимаем решение о наличии среднего потенциала Н3 в соответствии с Уровнями возможностей нарушителей по реализации угроз безопасности информации («Методика оценки угроз…»), так как, несмотря на наличие у «нашего» нарушителя широких исключительных знаний, практических навыков и специально разработанных средств оценки, данный вид нарушителя не имеет законных возможностей реализации угроз на физически изолированные сегменты систем и сетей – мероприятия мониторинга (оценки) проводятся исключительно в отношении информационных ресурсов органов (организаций), имеющих непосредственное подключение к информационно-телекоммуникационной сети «Интернет» и (или) сопряженных с сетью «Интернет» с использованием технологии трансляции сетевых адресов.

Приведем описание угрозы безопасности информации (УБИ) в нотификации Базы данных угроз ФСТЭК России.

Общие сведения.

Наименование УБИ – угроза нарушения функционирования (работоспособности) информационного ресурса, вызванного проведением мероприятий контроля (оценки) и мониторинга эффективности СЗИ.

Описание УБИ – частичная или полная утрата работоспособности или функциональности информационного ресурса.

Источник угрозы – внешний нарушитель со средним потенциалом.

DOI: 10.31854/2307-1303-2023-11-4-1-14
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/1-14.pdf

Объект воздействия – информационная система (информационный ресурс), имеющая непосредственное подключение к информационно-телекоммуникационной сети «Интернет» и (или) сопряженных с сетью «Интернет» с использованием технологии трансляции сетевых адресов.

Последствия: конфиденциальность – 0; целостность – 1; доступность – 1.

В связи с тем, что мероприятия оценки проводит уполномоченный сотрудник ФСБ России, допущенный до обработки информации ограниченного доступа, в законных целях, то считаем невозможным нарушение свойства безопасности информации «конфиденциальность», с установлением нулевого значения данного параметра при оценке последствий; нарушение же свойств «целостность» и «доступность» являются следствием частичной или полной утраты работоспособности или функциональности информационного ресурса (см. Описание УБИ).

Таким образом, сформировано описание «нового» типа угрозы безопасности информации, который будет актуальным в отношении органов (организаций), на которые распространяются Указ Президента РФ № 250 и приказ ФСБ России № 213.

Анализ возможных действий владельца информационного ресурса по нейтрализации «новой» угрозы безопасности информации

В данном случае органам (организациям) после актуализации модели угроз будет необходимо принять меры по нейтрализации «новой» актуальной угрозы. В силу требований приказа ФСБ № 213 органы (организации) не могут применить дополнительные технические меры защиты информации с целью недопущения воздействия на средства обработки информации (усиление СЗИ на период оценки). В силу требований приказа ФСБ № 213 органы (организации) не могут применить дополнительные технические меры защиты информации (усиление СЗИ на период оценки) и/или организационно-технические меры по обеспечению непрерывности критических процессов основной деятельности (предварительный анализ используемых методов и инструментов оценки, запрет на использование потенциально опасных при необходимости, проведение оценки в «технологические окна», обеспечение критических процессов основной деятельности на период оценки неавтоматизированными методами, проведение оценки в период планового прекращения выполнения критических процессов – ремонт, модернизация, техническое обслуживание). При этом для персонала органа (организации) установлены жесткие сроки восстановления функционирования информационных ресурсов в случаях наступления негативных последствий в ходе оценки – не более 6 часов.

Формально, произошедшие нарушения функционирования относятся к так называемым компьютерным инцидентам. И наиболее логичным следовало бы признать, что для обеспечения восстановления и минимизации последствий целесообразно действовать в рамках плана по реагированию на компьютерные инциденты и ликвидации последствий компьютерных атак. Но термин «компью-

DOI: 10.31854/2307-1303-2023-11-4-1-14
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/1-14.pdf

терный инцидент» законодательно введен только в отношении объектов критической информационной инфраструктуры, а планирование деятельности по реагированию на компьютерные инциденты предусмотрено только в части значимых объектов критической информационной инфраструктуры, что составляет незначительную часть оцениваемых информационных ресурсов органов (организаций) страны.

Анализ документов, регламентирующих планирование действий при реагировании на компьютерные инциденты, показал следующие особенности:

– значительная часть процедур, определенных государственными стандартами, носит избыточный характер для исследуемой ситуации;

– время, отведенное на мероприятия по реагированию и ликвидации последствий, планируется органом (владельцем) самостоятельно и никак не ограничено;

– пассивность – реагирование начинается только в случае выявления уже наступивших негативных последствий [12–16].

Но в требованиях по защите информации и обеспечению безопасности значимых объектов критической информационной инфраструктуры предусмотрено обеспечение действий персонала при возникновении нештатных ситуаций, которые носят проактивный характер[6] [17].

Анализ возможных действий владельца информационного ресурса по нештатной ситуации

Учитывая, что ФСТЭК России рассматривает компьютерные инциденты как частный случай нештатной ситуации, и тот факт, что задача по восстановлению работоспособности объекта информатизации проводится не специалистами (подразделениями) по защите информации, а эксплуатирующим персоналом, предлагается рассматривать мероприятия оценки в качестве нештатной ситуации для субъектов критической информационной инфраструктуры и государственных информационных систем, для иных информационных ресурсов органов (власти) в рамках планирования аварийно-восстановительных работ (АВР). Данный подход позволит реализовать почти единственное преимущество – точное знание периода времени, в который возможно возникновение негативных последствий. Получив в начале календарного года выписку из годового плана о проведении оценки, руководитель органа (организации) назначает ответственного исполнителя за подготовку плана АВР с учетом конкретных условий на плановые даты мероприятий по оценке. На роль ответственного исполнителя целесообразно назначать руководящий состав, отвечающий за непрерывность основных производственных процессов (главный инженер, главный энергетик и т. д.).

[6] Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

К основным мероприятиям подготовки к АВР можно отнести:

1) *оценку* влияния на основные процессы прекращения штатного функционирования информационных ресурсов (для объектов критической информационной инфраструктуры уже проведена при категорировании);

2) *расчет* сил аварийных бригад, сил обеспечения непрерывности основных производственных процессов без средств автоматизации, запасного имущества и принадлежностей;

3) *создание* внеплановых резервных копий программного обеспечения, запаса съемных машинных носителей информации, мобильных средств вычислительной техники и т. д.;

4) *определение* мест размещения ЗИП и резервных копий, обеспечивающих оперативный доступ аварийного персонала;

5) *организацию* резервных каналов связи, схемы аварийного энергоснабжения;

6) *заключение* рамочных договоров с внешними центрами технической поддержки;

7) *оповещение* клиентов о возможных перерывах при оказании услуг по договору;

8) *обеспечение* сил усиления служебным транспортом, местами размещения и отдыха;

9) *подготовку* пресс-релизов, документов для внеурочного привлечения работников, вызова из отпусков, изменения графика отпусков;

10) *мониторинг* средств массовой информации и социальных сетей для оперативного купирования репутационных потерь;

– и т. п.

В качестве методического обеспечения можно рекомендовать к рассмотрению и использованию ряд отечественных и зарубежных стандартов [12–14].

Анализ возможных действий сил информационной безопасности в нештатной ситуации

Роль подразделений информационной безопасности будет заключаться в проявлении так называемой должной осмотрительности. Орган (организация) может столкнуться с реальными компьютерными атаками в период проведения оценки. Это может произойти в двух ситуациях.

Первая ситуация – случайность. Простое совпадение в действиях ФСБ России и хакеров по времени воздействия на информационные ресурсы. Зная о проводимых мероприятиях, подразделения информационной безопасности органа (организации) могут принять действия хакеров за правомерные и не предпримут мер противодействия.

Вторая ситуация – целевая атака на орган (организацию) с использованием социотехнических методов. Перечень органов (организаций), в отношении которых может быть проведена оценка, является общедоступным. Процедура самой оценки не описана в документах и до органов (организаций) не доведена. Опыт прохождения такой оценки у органов (организаций) также отсутствует, поскольку

подобные мероприятия начнутся только в 2024 г. С учетом уже сложившейся практики целевых компьютерных атак, путем направления в органы (организации) фишинговых писем от имени ФСТЭК России[7], ФСБ России, НКЦКИ (https://safe-surf.ru/specialists/news/680267), Минцифры и Роскомнадзора (https://www.vedomosti.ru/technology/news/2023/12/06/1009663-roskomnadzor-predupredil-feikovoi-rassilke), в том числе о якобы проводимых в отношении органа (организации) проверки, мониторинга или уголовного расследования по компьютерным преступлениям, подразделениям информационной безопасности органа (организации) необходимо быть готовым к получению сообщений с почтовых адресов, маскирующихся под адрес электронной почты – monitoring@fsb.ru.

Заключение

Проведенный анализ действующих нормативно-правовых актов, национальных стандартов и практики их реализации при защите информационных ресурсов органов (организаций) показал невозможность противодействия (нейтрализации) угрозам безопасности информации, вызванных мероприятиями по оценке защищенности информационных ресурсов органов (организаций).

Представленный в настоящей статье подход к действию сил безопасности органов (организаций) призван минимизировать негативные последствия от реализации «нового» класса угроз за счет обеспечения готовности персонала органа (организации) к их возникновению и повышению эффективности АВР.

Реализация предложенного подхода по введению в руководящие документы ФСТЭК России «нового» типа угрозы безопасности информации позволит создать необходимую методическую базу обеспечения бесперебойного функционирования информационных ресурсов органов (организаций) Российской Федерации.

В дальнейших исследованиях планируется разработка методов и алгоритмов действий персонала, эксплуатирующего объекты информатизации, при возникновении нештатной ситуации и оценки эффективности предлагаемых решений по проведению АВР.

Литература

1. Цибизова Т. Ю., Панилов П. А., Кочешков М. А. Мониторинг безопасности системы защиты информации критической информационной инфраструктуры на основе когнитивного моделирования // Известия ТулГУ. Технические науки. 2023. № 6. С. 33–41. DOI: 10.24412/2071-6168-2023-6-33-41

2. Цыплакова А. Д., Шестак В. А. Участие местных органов публичной власти в совершенствовании мер профилактики кибератак в России // Государственная власть и местное самоуправление. 2023. № 2. С. 28–31. DOI: 10.18572/1813-1247-2023-2-28-31

3. Белов В. М., Пивкин Е. Н., Ардаева А. А. Комплексный подход к оцениванию защищенности значимых объектов критической информационной

[7] Информационное сообщение ФСТЭК России от 29.12.2023 № 240/22/6370.

инфраструктуры от несанкционированного доступа // Безопасность цифровых технологий. 2022. № 1(104). С. 9–26. DOI: 10.17212/2782-2230-2022-1-9-26

4. Захарченко Р. И., Королев И. Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52–61. DOI: 10.24411/2409-5419-2018-10041

5. Вечеркин В. Б., Галанкин А. В., Прохоров М. А. Методика оценивания устойчивости функционирования автоматизированной системы управления критической информационной инфраструктурой в условиях информационного воздействия // Известия ТулГУ. Технические науки. 2018. № 6. С. 160–170.

6. Максимова Е. А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 91–103. DOI: 10.31854/1813-324X-2020-6-4-91-103

7. Кузьмин В. Н., Менисов А. Б. Исследование путей и способов повышения результативности выявления компьютерных атак на объекты критической информационной инфраструктуры // Информационно-управляющие системы. 2022. № 4. С. 29–43. DOI: 10.31799/1684-8853-2022-4-29-43

8. Гаськова Д. А., Массель А. Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. № 2(30). С. 42–49. DOI: 10.21681/2311-3456-2019-2-42-49

9. Ан В. Р., Селифанов В. В., Табакаева В. А., Буларга С. А., Ворожцов А. С. Разработка методики аудита кибербезопасности ГИС, относящихся к объектам критической информационной инфраструктуры Российской Федерации // Сборник научных трудов НГТУ. 2019. № 3-4(96). С. 84–95. DOI: 10.17212/2307-6879-2019-3-4-84-95

10. Ан В. Р., Табакаева В. А. Разработка алгоритма проведения аудита кибербезопасности // 59-я Международная научная студенческая конференция (МНСК-2021, Новосибирск, 12–23 апреля 2021 г.). Новосибирск: Новосибирский национальный исследовательский государственный университет, 2021. С. 5.

11. Ситская А. В., Селифанов В. В., Звягинцева П. А. Вопросы аудита информационной безопасности // Безопасность цифровых технологий. 2023. № 3(110). С. 67–82. DOI: 10.17212/2782-2230-2023-3-67-82

12. ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762:2008) Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. М: Стандартинформ, 2011. 48 с.

13. ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования М: Стандартинформ, 2015. 28 с.

14. Planning Considerations for Cyber Incidents. Guidance for Emergency Managers. Federal Emergency Management Agency. 2023. URL: https://www.fema.gov/sites/default/files/documents/fema_planning-considerations-cyber-incidents_2023.pdf

15. ГОСТ Р 59711-2022 Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами. М.: Российский институт стандартизации, 2022. 16 с.

16. Майорова Е. В. Методические аспекты реагирования на инциденты информационной безопасности в условиях цифровой экономики // Петербургский экономический журнал. 2020. № 1. С. 155–162. DOI:10.25631/PEJ.2020. 1.155.162

17. Максимова Е. А., Буйневич М. В., Шестаков А. В. Проактивное управление информационной безопасностью субъектов критической информационной инфраструктуры как сложных организационных систем с динамически изменяющейся структурой // Вестник Воронежского института МВД России. 2023. № 2. С. 49–59.

Статья поступила 19 октября 2023 г.
Одобрена после рецензирования 25 декабря 2023 г.
Принята к публикации 25 декабря 2023 г.

Информация об авторах

Комаров Валерий Валерьевич – преподаватель АНО ДПО «Центр повышения квалификации «АИС», сертифицированный ведущий аудитор ISO/IEC 27001.
E-mail: vinnipux1@rambler.ru

Буйневич Михаил Викторович – доктор технических наук, профессор, ведущий научный сотрудник Управления организации научной работы и подготовки научных кадров Санкт-Петербургского государственного университета телекоммуникаций имени проф. М.А. Бонч-Бруевича.
E-mail: bmv1958@yandex.ru

Assessment and Monitoring of the Security of Information Resources as an Emergency Situation

Komarov V.[1], **Buinevich M.**[2]✉

[1]Center for advanced training «AIS»,
Moscow, 111123, Russian Federation
[2]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Formulation of the problem: *control (evaluation) and monitoring of the information protection system (IPS) effectiveness are an integral part of the protected information objects operation process (state information systems, information systems of personal data, significant objects of critical information infrastructure). Imperfection of the control and monitoring means of the IPS together with her the vulnerabilities often leads to computer incidents with protected informatization object subsequent failure and/or degradation of its. One of the effective ways to solve this problem is the organization and implementation of preventive measures.*

The purpose of the work *is reducing the response time and elimination of consequences from a computer incident caused by IPS measures to control (evaluate) the effectiveness.*

An additional goal *is to neutralize information security threats implemented by an external intruder using sociotechnical methods (fishing).*

Methods: *generalization and analysis of the existing regulatory and methodological support for the actions of information security units to carry out control (evaluation) measures, as well as in case of emergency situations and the occurrence of computer incidents.*

Novelty: *the novelty elements is consideration of the event on ISP effectiveness control (evaluation) as a non-emergency situation in the informatization object operation under protect.*

Result: *the necessity of introducing a threat to information security new class – the threat of information resource performance disruption caused by IPS control (assessment) and monitoring of the effectiveness are proved.*

Practical significance: *the results of the work can be used to ensure organizations information resources security when the Center for Information Protection and Special Communication FSS of and territorial security bodies in relation to them measures to assess their security and the ability of bodies (organizations) to resist threats to information security.*

Keywords: *information resources, information protection system, computer incident, external intruder, security monitoring and assessment, information security threat, abnormal (emergency) situation*

Information about Authors

Valery Komarov − teacher of the Autonomous non-profit organization of additional professional education «Center for advanced training «AIS», certified lead auditor ISO/IEC 27001. E-mail: vinnipux1@rambler.ru

Mikhail Buinevich − Dr. of Engineering Sciences, Leading Researcher at the Department of Scientific Work Organization and Scientific Personnel Training (The Bonch-Bruevich Saint-Petersburg State University of Telecommunications).
E-mail: bmv1958@yandex.ru

DOI: 10.31854/2307-1303-2023-11-4-1-14
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/1-14.pdf